IntechOpen

National Security in the Digital and Information Age

Edited by Sally Burt

National Security in the Digital and Information Age

Edited by Sally Burt

Published in London, United Kingdom

National Security in the Digital and Information Age
http://dx.doi.org/10.5772/intechopen.1005415
Edited by Sally Burt

Contributors
Adrian-Victor Vevera, Amit Lavie-Dinur, Chris J. Dolan, Haki Demolli, Hussain Syed Gowhor, Juraci Ferreira Galdino, Martin Kaloudis, Paulo César Pellanda, Romullo Girardi, Sally Burt, Ulpia-Elena Botezatu, Yuval Karniel

First published in London, United Kingdom, 2024 by IntechOpen
IntechOpen is the global imprint of INTECHOPEN LIMITED, registered in England and Wales, registration number: 11086078, 167-169 Great Portland Street, London, W1W 5PF, United Kingdom

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Additional hard and PDF copies can be obtained from orders@intechopen.com

National Security in the Digital and Information Age
Edited by Sally Burt
p. cm.
Print ISBN 978-0-85466-668-3
Online ISBN 978-0-85466-667-6
eBook (PDF) ISBN 978-0-85466-669-0

Meet the editor

Dr Sally Burt is lecturer in cyber security at the University of New South Wales, Canberra. She received her Ph.D. from the Australian National University in 2011, which focused on diplomatic history and Sino–U.S. relations. She brings this expertise to her research of the diplomatic context of cyber relations, the development of international cyber norms, the strategic use of information warfare and influence operations, information operations, and international interference. She has been published and has presented internationally on these areas. She also examines the use of cyber-enabled coercion and deterrence in conflict and as measures short of war. Sally is keen to promote deeper understanding of the human elements of cybersecurity and strategy and how they influence politics, diplomacy, and international relations.

Contents

Preface

National security has been a core function of states since their inception with the Treaty of Westphalia. The means of protecting national security have changed depending on the threat actors being faced, the nature of the nation being secured, the resources available to the state to secure its institutions and borders, and the strategy the nation chooses to follow.

The advent of the information age and the creation of networked and interconnected societies through digital transformation has led to challenges being posed to the ideas of the nation, borders, and sovereignty. National security and strategies, then, have also been reshaped, or are in the process of being redefined, to account for these deep technological changes.

Some strategies and tactics of national security that have been tried and tested over the ages are still employed by states around the globe, but in the digital age, the way these strategies and tactics are implemented can look a little different.

This book explores some of these older concepts of national security, such as sovereignty, the role of the state in security communications within their territory, and the means of conducting warfare and defining crime, but with the new context of the digital age and technologies creating a more interconnected globe. It also examines case studies of different states that are less commonly examined in the cyber context. This helps the reader develop an understanding of how national security is being thought about in the broader world and among smaller players.

This book also examines some new frontiers and areas where innovation is causing disruption, and the changes that it is likely to bring will impact more broadly than just within any one state. Partnerships between states and areas of potential cooperation are also examined within this volume.

Conflict in the cyber and information age will look very different from what has gone before. The world has a preview of what cyber and digital technologies will do to the battlefield in the information age, but the extent of those battlefields and how and where wars are likely to be fought is only just being imagined. It is hoped that this book will provide readers with the context of different issues facing states and the international community more broadly in the information age. This can lead to deeper thinking about the world in which we live, how secure we are, and what national security looks like, which is what this volume provokes.

Sally Burt
University of New South Wales,
Canberra, Australia

Section 1

Concepts of National Security

Chapter 1

The Gray Zone: Changing Our Understanding of National Security in the Information Age

Sally Burt

Abstract

This chapter will examine the changing understanding of national security in the cyber age, particularly with the development of an extensive Gray Zone. Gray Zone activities are now cyber-enabled and this has changed the nature of the Gray Zone. The boundaries of this zone are being bent and flexed. Until some firmer global norms and red lines are properly established by states in the international system, it will be difficult for behavior in the Gray Zone to be predictable or stable. Our contemporary understandings of effective deterrence and coercion in the international system are based on predictability, communication and signaling; aspects of the international system that are absent or at least very challenged in the information age. States that currently benefit from ambiguity in the Gray Zone seem to lack incentive to establish the norms and limits of their actions in a way that would lead to stability. The ability to utilize deterrence and coercion tactics effectively in the cyber age may be the unseen incentive provided from states with an interest in maintaining a rules-based order.

Keywords: Gray Zone, deterrence, cyberattacks, national security, United States

1. Introduction

Statecraft is defined as the skillful conduct of state affairs [1]. Promoting and protecting national interests and national security are the key aim of this activity. Each state will define its national interests differently and these interests will also change over time. The nature of conflict that challenges national interests is less changeable. War has been understood as the activity of armed conflict to achieve national interest, be it security and protection from others' aims or for facilitating a state's own aims by threatening another's. Military force is the heart of war. There has been some debate over centuries about whether the nature of war changes or can be changed by technology and the debates sparked by disagreement over this involve the idea of the Revolution of Military Affairs [2]. The key question being, does the nature of war change because of certain technologies and innovations or is it just the tactics used to conduct it that are altered? Even where there are successful arguments for the changing nature of war, the kinds of technological advancements that cause this are

very limited [2] and the number of times this has occurred through the centuries can be counted on one hand.

What is known as the Gray Zone, the statecraft that takes place that sits below the threshold of war is more changeable in nature. States conduct diplomacy, through espionage, sabotage, coercion, economic persuasion, and public diplomacy. The patterns and utility of each activity constantly changes according to the tools available to states, the most effective method of achieving the aim and the norms and taboos of diplomatic conduct as they change over time. The cyber age has brought some important changes to the way these activities are conducted and their effectiveness in achieving political interests. States are still adjusting to the utility of Gray Zone activities and developing understanding about how best to responds to cyber-based Gray Zone activities [3]. These matters are significant to international relations.

Current activity in the Gray Zone would suggest that states are struggling to define where red lines and thresholds of war are being crossed and some activities that could be seen as acts of war or provocation of conflict are being responded to with a much lower degree of response. This has potentially significant implications for the development of norms of *casus belli* in the future [3]. It also calls into question where the changed nature of the Gray Zone is leading to a rethinking about definitions of national security or the nature of war in terms of the way it is defined and conducted.

Through an examination of some of these changes, some key events and how they have been responded to, this chapter will examine these important questions and show that there is indeed some uncertainty about the role of war in statecraft in the cyber age.

2. The problem: defining the Gray Zone

The term "Gray Zone" can be traced to the US Special Operations Command paper written in 2015 [4]. It was used to describe the range of activities used in statecraft that can neither be defined as war nor peace, but rather as something in between. These are somewhat nefarious or malicious activities that do not present such a challenge to another state's national interests so that they should be considered an act of war. There is no exact definition of the Gray Zone and that is because the concept of national interests and the threshold for war differs between states [4]. Therefore, there is little capability to precisely label activities as being in the Gray Zone in any objective way.

This, however, does not mean, and should not preclude, states from determining what they consider Gray Zone activities as opposed to acts of war. In terms of breaches to a state's vital interests, it should be possible to know when an act is no longer a Gray Zone activity, but an act of war. There should be a clear line determining where the Gray Zone ends if not where it starts. States need to define their national interests and determine core/vital interests from within those broader interests to establish what is "acceptable" behavior by other states, even if it is not desirable. Within the confines of international law, states need to be able to recognize when their vital interests are threatened and a response and retaliation is warranted and legal. States then also need to determine how to respond according to the seriousness of this breach of national interests.

The process of determining these things must also account for international laws and norms, as relating to the declaration of war and what is considered a just *casus belli*. States are not entirely free to create their own definitions of when it is and is not acceptable to engage in war or what can be considered an act of war. They must

respond to the restrictions of the international community and international organizations designed to regulate (and try to avoid) war fighting [5]. International law also determines, to an extent, what reaction and activity will be considered by the international community to be an acceptable response to a given provocation [5].

An important question that must be posed, however, is are these restrictions outdated? Has the concept of war changed so that the Gray Zone is now the warfighting space? Or have states' determination of when it is "worth" going to war and what is "worth" fighting for changed?

Sovereignty is the key concept that underpins international law and the development of accepted norms of state behavior. It then also determines what should be *casus belli*. The clearest cut example of an acceptable *casus belli* in the international system is the invasion of another recognized state's territory. Under international law this would be the clearest violation of another state's sovereignty and a justification for war as a response in self-defense [6]. The issue in the cyber age is that borders no longer need to be breached with a military invasion for a state's sovereignty to be compromised. In this new age, technology allows states to cross borders for nefarious activity without physical presence and often without detection at all. The concept was not considered at the time of writing the United Nations Charter and much other international law. The issue of the applicability of international law to cyber activities and in this new age is well recognized. The Tallinn Manuals and various other fora have been established to consider these issues and provide some guidance on acceptable behavior in cyberspace [7]. The point here is not to rehearse these arguments around whether or not international law is keeping pace with technological change acceptably. Rather, the point is that states need to rethink their decision-making and understanding of their own sovereignty and national interests in the context of this new international environment in order to ensure they have appropriate strategies to deal with emerging threats in appropriate ways. Until this occurs, there is little basis for the development of strong international legal frameworks.

States need to understand what and when they consider their sovereignty to have been breached and their vital interests challenged and also what they should be able to do to protect themselves in different circumstances. This understanding will lead to the possibility of better and clearer negotiations on state behavior and also ensure that the hard international law is supported by acceptable norms. In this way, the Gray Zone in the cyber age will be more clearly defined also. There will be less room for ambiguity and, therefore, greater stability in international relations. Transforming the Gray Zone into normal statecraft short of war will ensure that unacceptable or accidental war is more likely to be avoided.

3. Changing old concepts

The last decade or so, as the implications of cyber technology and capabilities were becoming more visible and apparent due to the increase in cyberattacks being conducted, debate has arisen over whether old theories of strategy and war fighting are relevant or hold in the new cyber-enabled international system. Many scholars have questioned the applicability of concepts such as Douhet's airpower theory, Jomini's fighting at the decisive point, or Clausewitz's principles of war and even Sun Tzu's Art of War to the cyber age and the conduct of international relations using this technology [8–10]. There has also been work done on how small wars alter Grand Strategy through the shifting of power and elements within the international

system [11]. It could be argued that this same process is operating through the cyber domain with different interactions and attacks slowly shifting the power relations and other elements of the international system in ways that lead to changes in the Grand Strategy of states. Certainly, cyber technology has caused a great deal of thinking and debate about these matters and about how states should interact with each other. The Gray Zone may be being used as a testing ground for future behavior and norm development and ultimately patterns formed around these interactions will lead to the resolution of at least some of these debates [3].

The scholarly debate and questioning of old strategies reflects the observations about the different ways in which cyber technology has impacted long held and understood concepts and tactics of diplomacy and statecraft. Some of these changes are examined below.

3.1 Public diplomacy

Public diplomacy is the concept of a state conducting diplomacy with the public of another [12]. Where "normal" diplomatic relations are conducted between officials from their respective governments, public diplomacy involves bypassing these officials and "speaking" directly with the society of another state. Public diplomacy is not a new practice, it has been a way for states to persuade another state of its virtues and to gain support for its policies and decisions through direct engagement with the people. Winning over the public is an effective mechanism for gaining persuasive power over another state, particularly a democracy. Public diplomacy is very closely related to soft power and it is about promotion of ideas and policies and convincing the society of another state of their worth [13]. Traditionally, the media, including newspapers and radio have been used for this purpose. State officials have also been known to make public appearances and make speeches that are broadcast for the consumption of the public in another state.

The internet and social media have brought innovation to this age-old concept. Using these technologies has increased the range, speed and breadth of the ability to communicate directly with people in another country. It has also allowed an element of anonymity to come into this concept. One of the key facets that makes public diplomacy an acceptable activity allowed by most governments is the fact that it is known who and how the communication with their publics is transpiring [14]. The advent of the internet and social media has removed this element of this form of statecraft. States can now be quite anonymous and spread messages in a much less transparent way. This presents a danger in that it can lead to a shift from public diplomacy into a Gray Zone tactic that is more nefarious, information or political warfare. Crossing the line of the threshold of hostility without necessarily causing conflict.

3.2 Coercion

Coercion is another tool of statecraft that has long been used by states to engage with each other and to seek out their own interests. In the cyber age, however, there have been differences made to the use of this tool that are important to interstate relations and the identification and protection of national interests.

Coercion is commonly used to refer to the idea of the use of force or threat of the use of force to influence another state's behavior. It is often used to mean a combination of the idea of deterrence (or the prevention of activity) and what Thomas Schelling referred to as Compellence or providing incentive to undertake an activity [15].

Coercion has a long, long history in international relations and statecraft. The means by which states coerce others into behavior more aligned to their own interests changes constantly and is very much situationally dependent [16]. The severity of the force threatened, or used to support the credibility of the threat, also changes according to the interests in the behavior change and the severity of outcomes for the coercer should the behavior remain unchanged.

In order to determine how cyber has altered the nature of this tactic of statecraft, it is important to understand the concept of "force" and how we define that term. If we consider force purely to mean kinetic and traditional forms of military force, then we severely limit both our conception of how cyber tools can be used for this activity and also our recognition of when a state is coercing another. Economic coercion can be used to amend another state's behavior just as much as military force. It is the pain that is caused that creates the incentive to alter behavior [17] and so we need to consider the idea of force more loosely so that we allow for different means for coercive behavior to be understood, particularly in the current cyber context. Where cyberattacks and cyber tools can be used to cause pain to an opponent and to degrade something of value to them, then cyber coercion can occur [16]. As will be seen below, sometimes cyber tools are also used in ways related to both military, diplomatic and economic coercion.

Cyberattacks have been used in recent years as an effective coercive tool. The reversibility of the impact of certain types of attacks makes them ideal for punishing a state's behavior and then being able to remove that punishment once the behavior has been altered. The cyberattack on Sony Pictures is an example of the use of cyber tools for coercive purposes. The November 2014 attack on Sony Pictures was attributed to North Korea and involved an attack on the movie company because of its production of a film *The Interview* that was offensive to the North Korean leadership [18]. In order to prevent the movie's release, North Korea engaged in cyberattacks on the company that included gaining access to data about scripts and unfinished films etc., the release of which would be damaging to Sony's profits. Sony was held to ransom with the threat also of September 11 style terrorist attacks in cinemas that showed the movie. The film's release was duly postponed and even when it was released, this was done on a much smaller scale than originally planned [19].

Another example of the possible use of cyberattacks for coercion occurred in an attack on the Australian Parliament and government agencies in 2020 after Australia called for an inquiry into the origins of COVID-19. There were also other tensions in relations between China and Australia at the time. The attacks targeted a range of private sector organizations as well as political and government agencies. Although the attacks were not officially attributed to China, it is widely believed that they were the perpetrators of the attack. It also fits with the probably coercive intent. When factoring in which state had the most potential benefit from the attacks and the timing of the attacks, China makes sense as the perpetrator with coercion as the motive [20].

Cyber tools also make the possibility of coercing with less risk of escalation more feasible and, therefore, potentially more common. Coercion is arguably more effective with a reversible impact because the coercer can actually demonstrate their ability to implement the threatened imposition of cost and then remove it. The damage from more traditional force is not often as easily reversible. The implications are that cyber technology has also expanded coercion opportunities and capabilities to states that may otherwise not have had sufficient ability to threaten the power of another militarily superior state [16]. It provides an asymmetric advantage to less powerful states and also potentially non-state actors.

More discreet forms of coercion with cyber tools come in the form of what might be defined as part of political or information warfare. With cyber means, there is a greater possibility to undertake deceptive or covert coercion through the persuasion and influence over a foreign population [16]. Democratic states are most susceptible to this in that public opinion is a significant influence on policies and government decisions in these states. Authoritarian regimes, however, are not immune. One of the biggest vulnerabilities of authoritarian regimes is controlling information accessed by the population in order to maintain control. The concept of nefariously interfering with another state's population to disrupt the decision-making processes of the government is not a new tactic or activity, but cyber technology has enhanced the capability in terms of potential reach of messaging and influence and also the ability to do so without being detected or having the intent of the activity revealed [16].

3.3 Deterrence

Deterrence is a form of coercion that is based on the prevention of a behavior encouraging another state to stop a behavior they are engaging in [21]. There are several forms of deterrence and these are effective in different scenarios.

There is deterrence by punishment. This type of deterrence can be used to reverse a behavior that has already been undertaken or use the threat of such punishment (with a credible backing of a state's capabilities and will to carry out the threat) to prevent a behavior occurring. The idea is that a state will punish or punishes the behavior and so the outcomes for the state to be deterred will be so costly or damaging that, again, undertaking or continuing the behavior is irrational as the benefit of achieving the aims and interests sought is outweighed by the costs [22]. It relies firstly on rational decision-making and secondly on an ability to accurately calculate the cost of the outcome in relation to the benefit of non-compliance. The second of these conditions is harder to meet in the cyber age with the impact of cyber attacks being harder to determine, particularly in the idea of damage and cost imposition. It is also harder to build credibility as a coercer because of a lack of track record in cyber based attacks and responses and also the guarded secrets about a state's cyber capabilities.

There is also deterrence by denial. The idea behind this type of deterrence is that the opponent or target of the deterrence needs to be convinced that continuing the behavior (or undertaking it in the first place) that a state is trying to deter will not result in the achievement of its aims or interests. Continuing or undertaking the action is then redundant and counter productive because it will not achieve the aims or benefit the state and this action would be irrational [22]. Again, in the cyber age the elements of a deterrence tactic that are necessary for its success, including the ability to signal how the deterring state would deny the opponent achieving its objectives are harder to implement in cyberspace.

In the cyber age, there has been a good deal of scholarly debate about the efficacy of deterrence as a tool of statecraft. According to Borghard and Lonegran, scholars who have promoted the idea that deterrence cannot work in cyberspace have been overly pessimistic. They claim that although deterrence by punishment is not very effective because of the unique features of interactions in cyberspace, deterrence by denial can be much more effective if properly understood and applied [10]. In a related argument, Uri Tor claimed that lessons from the idea of "cumulative deterrence" used by Israel in response to its neighbors could also be a more effective way to think about the applicability of deterrence in a cyber-enabled environment. The idea of cumulative deterrence is that deterrence does not happen as a one off interaction

that prevents a nuclear attack, as was the common use of the model in the Cold War period, but rather it is an ongoing process of "training" the behavior of the opponent through multiple interactions and the pattern of response [23].

One of the major reasons that scholars provide for the lack of effectiveness of deterrence in cyberspace is the lack of ability to attribute attacks and actions. This view is becoming outdated as attribution capability improves in both a technical sense as well as in the ability to identify interests being served by attacks and the ability to deduce likely perpetrators becomes a more acceptable threshold of attributing incidents [24]. That is, our understanding of the specificity of the attribution and how the claims are made has matured and developed over time in favor of looser attribution. This is not to say that random and unjustified naming and shaming of a state would be tolerated, but neither is there a need to be able to prove without a shadow of a doubt who was behind the attack, matched by the evidence levels of technical elements of the attack and who undertook it [24].

Ultimately what is more detrimental to the effectiveness of deterrence in cyberspace is the ambiguity of a range of features. Firstly, states have been slow to develop "Red Lines" [23]. That is, states are not making the point of signaling when another state is pushing the edges of Gray Zone towards war. Without a clear understanding of an opponent's red lines and vulnerabilities and pain points, implementing a deterrence strategy is very difficult. Communication is key to this understanding and arguably, this communication is lacking in the international system in the cyber age for a variety of reasons. Secondly, and relatedly, many states seem unprepared or reluctant to develop rules of the road for cyber interactions either explicitly by rejecting negotiations of international agreements or implicitly through failure to retaliate for attacks, even for attacks that seem to warrant a serious response. More on this later.

3.4 Trade

States can also utilize trade relations and mechanisms to engage with each other and to pursue their national interests. Although trade relations are seen as beneficial to states, as they promote commercial activities and stimulate economies, they can be disruptive or concerning for various reasons.

Firstly, even in what may appear on the surface a positive trade relationship, some states can be exploited by others. Any commercial arrangement or trade agreement can be written to benefit one side more than another. They will reflect the relative power relationship of the two states as well as their economic strength [25]. This is the case in cyber and non-cyber trade relations. The need to be connected and to have access to the latest technology in order to compete in a global economy that is driven by innovation and connectivity can be additional incentive for states with less indigenous cyber industry or ability to afford this technology to accept one-sided deals. There can be deliberate attempts to create trade relationships that are deeply one-sided and ill designed for mutual benefit as well as this being a more accidental result. This can be used as a form of economic coercion [26].

Secondly, there can be national interest and security concerns that arise from the nature of the product being sold. In the cyber and information age, this has become a large and growing problem. In the case of cyber technology being traded, however, there can be hidden traps in terms of a lack of standards, the inclusion of spyware on applications provided in a trade providing access to possibly sensitive information that another state could use maliciously [26]. States may be unaware of what

technology or software can do and how other states will use access to their vital state functions through different technology and software that is traded. There is a greater capacity to deceive in cyberspace through trade relations than is generally the case in trade and commercial activity in tangible goods and more familiar services [27]. National security can be challenged in undetected and undetectable ways through cyber means making trade a more threatening activity than in the pre-cyber world.

Cyber technology and its application to tactics of statecraft have changed the nature of what were generally considered to be normal and acceptable interactions between states and of conducting international relations to be potentially much more threatening to national security. The nature of the Gray Zone, then, has also changed and become a more threatening environment in which states operate. Activities that were once considered acceptable may no longer be so benign, creating the problem or redefinition of the Gray Zone that was already hard to define.

4. Determining the thresholds of war

In order for states to be able to ensure their national interests are being protected in this new environment of conflict and state competition, decisions need to be made about what the thresholds of war are in this new context. To do this, the nature of war in this environment also needs to be understood from the point of view of engagement in war as an activity to help achieve a state's interests and from the concerns around escalation of competition and conflict from the Gray Zone and into an outright war scenario and what the likely consequences of such actions would be.

A sensible and rational decision about what was worth risking war over is easier when there is a clear understanding about the nature of war, weapons, conflict, others' interests and intents as well as what is likely to lead to escalation. There is also an element of determining the relative power of both sides and what they are likely to be able to achieve militarily from a kinetic conflict [28]. In the world of more traditional war and kinetic conflict it was much easier to determine these factors that lead to rational calculations on which to base decisions about war. In the cyber age, there is less understanding about each of these factors. What damage can be done with cyberattacks? How can that damage be measured in terms of tangible outcomes? Even the interaction between kinetic and traditional warfighting capabilities and weapons is hard to determine and understand. Measuring another state's power in terms of its cyber capabilities is, therefore, also difficult.

Traditionally, decisions about power and relative strength of states, that have also been the basis for rational calculations about going to war, have defined power in terms of kinetic military strength. The quantum of arms was a relatively easy measure, though not necessarily a straight one to one calculation of certain weapons. Generally, though, the destructive capability of a weapon could be determined, measured and the capacity of weapons could also be determined and compared between militaries and states [29]. National power, then, was somewhat measurable. Of course, complications such as a state's ability to mobilize it population, the motivations for war and the political strength of a leader or leadership to bring the will of its population to bear on a decision to go to war also mattered and were far less tangible.

Cyber power and the capability of cyber weapons is not so measurable as kinetic weapons and traditional military strength and capability [29]. Not only is the destructive capacity of a cyber weapon less straight forward, but the understanding of how combinations of different cyberattacks interact with each other and how much

disruption can be caused is lacking among the general population of many states. The reversibility of damaged caused by cyberattacks also makes this calculation of destruction and power less certain.

Cyber is not the only new capability that has led to a rethink about states' national interests and what should be defined as vital interests or not [21]. In the nuclear age, as the ultimate escalation threat became the destruction of humankind, there was a need for states to rethink what it was they were prepared to go to war over [30]. As Clausewitz made clear, once a conflict has begun, controlling escalation is not always possible [31]. Much of the Cold War was spent strategizing ways to prevent or manage escalation, certainly to avoid at least this ultimate destruction. Deterrent signaling and proxy wars became the predominant strategy of the latter Cold War period [32]. Although as scholars have pointed out, not all our learnings from nuclear deterrence are helpful to understanding how deterrence could and should work in the cyber age [9], but surely the lessons about avoiding and managing escalation should be carefully considered in the context of cyber-enabled conflict.

If national power and capability is more difficult to calculate, then the rationality of decisions about warfighting and defense of national interests can also be called into question. The value of national interests also need to be considered. A state needs to be to able to accurately assess its relative power and strength in order to be able to determine how much it can value a particular interest [21]. If it is not capable of defending itself against another state, then it must capitulate when challenged. If it has some power to defend itself against certain levels of attack or those from certain opponents, then it can make decisions about what it will risk in terms of defending different interests. In the cyber age that capability and relative power is harder to determine and it also gives greater strength to unexpected states [22]. The example of the Ukraine's resistance to Russian attacks in recent years is a clear example of the shifting power balance in the international community in the cyber age. It also potentially demonstrates the inaccurate assessment of national power.

In democratic states, there are checks and balances on decisions to go to war that also need to be factored into this decision. The will of a state to contest for its national interests is, in part, determined by the ability to sustain support from the population. The population ultimately bears the cost of the war and provides the resources with which to fight it. Governments in democracies, then, are constrained by public sentiment as well as their collective assessment of the value of the national interest [33]. The wars in Afghanistan and Iraq over the decades since the turn of the century provide an instructive example of the value populations place on national interests and security and the impact that can have on war fighting. It is particularly illustrative of the consequences of governments and populations having mismatches in understanding of the value of different national interests and the need to defend them through war [34]. The Gray Zone may then be the only available ground on which to fight.

Some states have a vested interest in retaining, if not increasing, the ambiguity of the Gray Zone. For those undertaking quite nefarious and malicious activity aimed to threaten even vital national interests under the guise of what were once normal and acceptable activities statecraft, it is good to have the cover of the Gray Zone from which to operate. States with less traditional military power or kinetic capability with which to influence the international system and protect their national interest can operate quite effectively in the Gray Zone in a way that causes significant damage to another state's national interests [3]. The problem is that this turns the Gray Zone into

the war zone. Allowing this to occur without response or understanding of what is happening can lead to unintended loss of national sovereignty and erosion of national security and power.

5. Redefined war or redefined national security

An important issue to be resolved for states, then, in this cyber age, it has the nature of war changed or does it remain the same but with new weapons? Whatever the answer to that question, a related one needs also to be addressed, which is do we need to redefine our understanding of national security?

When we understand the context of decision-making and war resulting from clear answers to these two questions, then we can better define what is considered to be the Gray Zone. Or acceptable measures of statecraft that are short of war. Behavior states are happy to accept from other states without responding with war to address defines where the threshold of war lies and the Gray Zone ends.

It seems, however, that the current thresholds for war, particularly in response to cyberattacks, are quite high. The United States in recent times has seemingly accepted quite a lot in terms of vital interests being attack with minimal response, and certainly not a war. Russian attacks on the 2016 and 2018 elections that were designed to sway the outcome and seemingly interfered with the ultimate condition of sovereignty of the United States, the electoral process, did not provoke war. The US seems to have preferred to deal with these breaches with a doubling down on its ability to protect its institutions from future attacks than with retaliating (at least directly) to those already undertaken [35]. There is a need to caveat this claim with the possibility of things being done in the classified space unknown to the general public and unavailable for analysis.

Another attack posing a seemingly significant challenge to US sovereignty or vital national interests was the Chinese attack on the Office of Personnel Management in 2014–2015. The attack was a massive data breach that saw access gained to some 21.5 million Americans' personal and sensitive data that was in the system for security clearance checks [36]. This was a very serious attack and the Obama Administration admitted it was such. The response to this was also to focus on improving US cyber defenses rather than punishing the perpetrators [37]. This was early days in the engagement of state sponsored cyberattacks and so it could be that a lack of understanding of how to respond appropriately may excuse relative inaction on the part of the Obama Administration. It may also be noted that this was an act of espionage and not an open attack on key sovereign functions of the United States government. Nonetheless, this was a serious attack on fundamental aspects of US national security.

It seems from the response to these attacks and the pattern being set of retaliation for challenges of this kind, which has continued in more recent years, that states, at least for now, are happy operating in the Gray Zone. For longer term norm development about crossing thresholds for war a rethinking of what it means to defend one's national security may need to occur or eventually action will need to be taken against a state clearly breaching another's sovereign rights. It may be that the concept of sovereignty needs to be redefined in the cyber age given how easily borders can be penetrated and foreign populations reached. If states are perpetually operating in the Gray Zone, even in ways that would traditionally have been thought of as the engagement in acts of war, then it will cease to be a Gray Zone and the nature of what was considered war will have changed. Where national security is gravely threatened in the Gray Zone and retaliation for those acts occur there also, the Gray Zone will have become the war zone.

6. Conclusion

The cyber age has presented challenges to concepts and activities in international relations that states thought were long settled. Cyber technology and the capabilities it brings have led to a questioning of the applicability of existing international law and norms. Bigger and more fundamental concepts such as what is meant by national security and where the threshold between the Gray Zone and war lies are also in need of rethinking. While states suffer from the impacts of cyberattacks and other Gray Zone activities that threaten different aspects of national security and retaliate without determining where the threshold of war actually lies, the Gray Zone remains the epicenter of the conduct of malicious international relations.

States need to give due consideration to the precidents being set and the patterns being established that impact the effectiveness of deterrence and coercion in the cyber age. Without clear red lines and declared thresholds for war, the Gray Zone remains an unstable and dangerous environment in which to conduct international relations. It may be that a transition is occurring that involves the rethinking of what is meant by national security and vital national interests and how they are defended. Or it may be that states are grappling with new tactics and means of engaging in conflict that remain (at least for now) in what is considered the Gray Zone. If that transition and rethinking are not happening blindly and states are indeed making conscious decisions about these concepts, then clear strategy is being applied. If, however, states are fumbling through without clear plans and recognition of the processes occurring in the security and international relations environment, then it is indeed a dangerous space in which the world is operating. Hopefully, if the latter is the case, an awakening will occur before it is too late.

Conflict of interest

The author declares no conflict of interest.

Author details

Sally Burt
University of New South Wales, Canberra, Australia

*Address all correspondence to: s.burt@unsw.edu.au

References

[1] Soanes C, Stevenson A. Oxford Dictionary of English. 2nd ed. Oxford: Oxford University Press; 2003

[2] Fissel M, editor. The Military Revolution and Revolutions in Military Affairs. Berlin, Boston: De Gruyter Oldenbourg; 2023. DOI: 10.1515/9783110661415

[3] Wirtz J. Life in the "Gray Zone": Observations for contemporary strategists. Defense and Security Analysis. 2017;**33**(2):106-114

[4] United States Special Operations Command White Paper: The Gray Zone. 2015. Available from: USSOCOM-GrayZones.pdf (publicintelligence.net)

[5] Smith P. Cyberattacks as casus belli: A sovereignty-based account. Journal of Applied Philosophy. 2018;**35**(2):222-241

[6] Macedo S. Introduction. In: Doyle M, editor. Striking First: Preemption and Prevention in International Conflict. Princeton: Princeton University Press; 2008. pp. xi-xxiv

[7] Schmitt M, editor. Tallinn Manual on the International Law Applicable to Cyberwarfare. Cambridge: Cambridge University Press; 2013. DOI: 10.1017/CB09781139169288

[8] Greathouse C. Cyberwar and strategic thought: Do the classical theorists still matter? In: Kremer J-F, Muller B, editors. Cyberspace and International Relations. Berlin: Springer-Verlag; 2014. pp. 21-38

[9] Fischerkeller M, Harknett R. Deterrence is not a credible strategy for cyberspace. Orbis. 2017;**61**(3):381-393

[10] Borghard E, Lonegran S. Deterrence by denial in cyberspace. Journal of Strategic Studies. 2023;**46**(3):534-569

[11] Lissner R. Wars of Revelation. Oxford: Oxford University Press; 2021

[12] Gregory B. American public diplomacy: Enduring characteristics, elusive transformation. The Hague: Journal of Diplomacy. 2011;**6**(3/4):353

[13] Nye J Jr. Soft power and American foreign policy. Political Science Quarterly. 2004;**119**(2):255-270

[14] Mazumdar T. Digital diplomacy: Internet-based public diplomacy activities or novel forms of public engagement? Place Branding and Public Diplomacy. 2024;**20**:24-43

[15] Van Angeren J. The opportunities and limits of compellence strategies [thesis]. Netherlands: Leiden University; 2006

[16] Valeriano B et al. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford: Oxford University Press; 2018

[17] Schelling T. The diplomacy of violence. In: Art R, Waltz K, editors. The Use of Force. 2nd ed. Lanham: University Press of America; 1983. pp. 101-122

[18] Peterson A. The Sony pictures hack, explained. Washington Post. 2014. The Sony Pictures hack, explained - The Washington Post

[19] Associated Press. North Korean programmer charged in Sony hack, Wannacry attack. PBS News. 2018. North Korean programmer charged in Sony hack, WannaCry attack | PBS NewsHour

[20] Hurst D. Cyber-attack Australia: Sophisticated attacks from 'state-based actor', PM says. The Guardian. 2020. Cyber-attack Australia: sophisticated

attacks from 'state-based actor', PM says | Australian security and counter-terrorism | The Guardian

[21] Snyder G. Deterrence and Defense: Toward a Theory of National Security. Westport Connecticut: Greenwood Press; 1975

[22] Nye J Jr. Deterrence and dissuasion in cyberspace. International Security. 2016/7;**14**(3):44-71

[23] Tor U. 'Cumulative deterrence' as a new paradigm for cyber deterrence. Journal of Strategic Studies. 2017;**40**(1-2):92-117

[24] Blagden D. Deterring cyber coercion: The exaggerated problem of attribution. Survival. 2020;**62**(1):131-148

[25] Lillich R. Economic coercion and the "new international economic order": A second look at come first impressions. In: Lillich R, editor. Economic Coercion and the New International Economic Order. Virginia: The Michie Company; 1976. pp. 107-122

[26] Benchea L. Impact of digitalization on economic diplomacy: Mega-trends and opportunities. The Romanian Economic Journal. 2023;**26**(85):13-20

[27] Huang K, Madnick S, Zhang F. Varieties of public-private co-governance on cybersecurity within the digital trade: Implications from Huawei's 5G. Journal of Chinese Governance. 2021;**7**(1):81-110. DOI: 10.1080/23812346.2021.1923230

[28] Ayson R. Thomas Schelling and the Nuclear Age: Strategy as Social Science. London: Frank Cass; 2004

[29] IISS. Cyber Capabilities and National Power: A Net Assessment. Research Paper. 2021. Cyber Capabilities and National Power: A Net Assessment (iiss.org)

[30] Art R, Waltz K. Technology, strategy, and the uses of force. In: Art R, Waltz K, editors. The Use of Force. 2nd ed. Lanham: University Press of America; 1983. pp. 1-32

[31] Paret P. Understanding War: Essays on Clausewitz and the History of Military Power. Princeton: Princeton University Press; 1993

[32] Yaacov B. The strategy of war by proxy. Cooperation and Conflict. 1984;**19**(4):263-273

[33] Kutz C. On War and Democracy. Princeton: Princeton University Press; 2016. DOI: 10.1515/9781400873937

[34] Shortridge A. The U.S. War in Afghanistan Twenty Years on: Public Opinion Then and Now. The Water's Edge; 2021 The U.S. War in Afghanistan Twenty Years On: Public Opinion Then and Now | Council on Foreign Relations (cfr.org)

[35] Landay J, Lewis S. US Intelligence Report Alleging Russia Election Interference Shared with 100 Countries. 2023. US intelligence report alleging Russia election interference shared with 100 countries | Reuters

[36] Oversight Committee. The OPM Data Breach: How the Government Jeopardized our National Security for More than a Generation. Report. 2016. Available from: oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[37] Nakashima E. Hacks of OPM databases compromised 22.1 million people, federal authorities say. Washington Post. 2015

Chapter 2

Digital Sovereignty as a Weapon of Diplomacy in Cyber Warfare in Democracies

Martin Kaloudis

Abstract

As our world becomes more digitally entwined, the concept of digital sovereignty has emerged as a critical determinant in international diplomacy. This chapter scrutinises the significance of digital sovereignty amidst rising cyber conflicts, showcasing its dual nature as both a defensive strategy and a diplomatic instrument. By exploring the interplay between traditional diplomatic practices and the evolving digital threat landscape, it sheds light on the intricate challenges and opportunities faced by nations. As states grapple with the complexities of safeguarding their digital borders while navigating diplomatic engagements, understanding the nuances of digital sovereignty becomes paramount in maintaining geopolitical stability and security in an increasingly interconnected global arena.

Keywords: digital sovereignty, cyber war, diplomacy, cyber attacks, cyber resilience, international relations

1. Introduction

The beginning of the twenty-first century marks a significant change in diplomacy influenced by the widespread use of digital technologies and the prevalent role of digital media in global affairs. This major change has transformed how countries interact and has required a rethink of conventional ideas about sovereignty, resolving conflicts and related diplomatic tools. Central to this evolving landscape is the concept of digital sovereignty, denoting a state's capacity to assert strategic autonomy over its digital infrastructure and data assets. It encompasses the ability to make independent decisions and undertake actions that uphold and safeguard state sovereignty in an increasingly interconnected digital realm.

This chapter embarks on an in-depth exploration of the multifaceted role of digital sovereignty as a diplomatic tool in the context of cyber conflicts. It delves into how digital sovereignty serves as a linchpin in countering cyber threats, mitigating the risk of conventional warfare and advancing national interests on the global stage. By elucidating the intricate interplay between digital sovereignty and diplomatic strategies, the chapter sheds light on the pivotal role of digital diplomacy in navigating the complexities of the digital age. Through a nuanced analysis of case studies and

theoretical frameworks, it seeks to uncover the underlying dynamics shaping contemporary diplomatic practices in the face of evolving digital threats and opportunities.

Furthermore, the chapter examines how digital sovereignty can serve as a catalyst for innovative approaches to conflict resolution and peacebuilding in the digital era. By harnessing the power of digital technologies and leveraging diplomatic channels, states can forge consensus, build trust and foster cooperation to address cyber conflicts and promote regional and global stability. Through a synthesis of theoretical insights and practical examples, the chapter offers a comprehensive understanding of the strategic imperatives and diplomatic nuances inherent in the pursuit of digital sovereignty in an age of digital disruption.

In essence, this chapter serves as a roadmap for policymakers, diplomats and scholars grappling with the complexities of diplomacy in the digital age. It underscores the imperative of embracing digital sovereignty as a cornerstone of contemporary diplomatic practice, while also illuminating the potential of digital diplomacy as a means to navigate the challenges and opportunities presented by the digital revolution. By embracing digital sovereignty as a guiding principle, nations can chart a course towards a more secure, stable and prosperous global future in the digital era.

2. Methodology

This study commences with an exploration of the dynamic intersection of diplomacy, cyberspace, digital sovereignty and digitisation, particularly in the context of current geopolitical challenges. Striving for a balance between accessibility and scholarly rigour, the analysis employs both qualitative and quantitative methods to bring these abstract concepts into a measurable realm. It is underpinned by a thorough review of existing literature and an examination of available secondary data.

Central to this study is the role of cyber resilience and digital sovereignty as emerging tools in the diplomatic toolkit. These concepts are subjected to a detailed quantitative analysis, including linear regression, to uncover potential relationships and causal links. This approach not only provides clarity but also enhances our understanding of how these concepts interact within the broader geopolitical landscape.

The analysis uses state rankings in index comparisons, valuing their stability against outliers. More complex statistical methods, such as Spearman and Pearson coefficients, are used, their inclusion offers additional insights in statistical correlations.

Additionally, this research includes a historical analysis to illustrate the evolving role of digital sovereignty in diplomacy. This part of the study provides a contextual backdrop, showing how diplomatic tools have adapted and evolved in response to the digital revolution.

3. The concept of diplomacy in the context of cyber attacks

The traditional concept of diplomacy, understood as the conduct of negotiations and the conclusion of agreements between states, is being expanded by digitalisation. Cyber warfare, the use of digital attack tools, such as phishing or malware, to harm another state or, in the sense of a counterattack, hackbacks to defend against cyber attacks, represents a new form of warfare that poses new challenges for diplomacy [1]. The boundaries between conventional warfare and cyber warfare

are becoming blurred, making new diplomatic instruments and strategies necessary. Defence organisations in many NATO states have, therefore, long since created so-called dimensions to defend against attacks in cyberspace in addition to air, naval, army and space units [2].

Diplomacy in its traditional form is understood as the art and science of conducting negotiations between representatives of different groups or states. Its primary function is to prevent conflicts and their escalation. This disciplined approach, which is deeply rooted in historical traditions and established rules, aims to address common problems, balance interests and resolve conflicts in a peaceful manner [3].

The origins of diplomacy date back to ancient Egypt and the Middle East in the fourteenth century BC. Modern diplomacy, however, has its roots in the relationships that developed between the Italian city states in the thirteenth century. This historical development shows how diplomacy has evolved over the centuries from simple interstate interactions to a complex system of international relations.

In the modern world, diplomacy plays a crucial role in shaping international relations, building understanding and cooperation and avoiding conflict. It encompasses a wide range of activities from formal negotiations and treaties to informal talks and cultural exchanges. The evolution and continuing influence of diplomacy on global politics demonstrates the importance of this field in maintaining international stability and peace. Modern diplomacy manifests itself not only in bilateral interactions between two states but also extends to multilateral platforms, such as the United Nations (UN), where it plays a key role in global political dynamics [3]. The objectives of this diplomacy are diverse and complex. They include the promotion of national interests, with diplomats acting as representatives and protectors of the political, economic, cultural and other interests of their home country. A key objective is peacekeeping, whereby conflicts are avoided or resolved through dialogue and negotiation, which contributes to global stability. Furthermore, diplomacy serves to build and maintain long-term relationships between countries and cultures in order to promote understanding and cooperation. The exchange of information also plays an important role as diplomats collect and exchange information relevant to the political decision-making of their home country. Last but not least, diplomacy involves conducting negotiations on treaties and agreements that regulate relations between countries. These instruments of diplomacy apply equally to the prevention of conventional, hybrid and cyber threats.

In the context of an increasingly digitalised and interconnected world, cyber diplomacy is gaining in importance. It deals with the use of cyberspace for diplomatic purposes and the management of conflicts and challenges in digital environments, that is, those that are made possible by cyberspace and is therefore relatively new [4]. It represents a state's efforts to seek a basis for negotiation with a potential adversary in order to avoid protracted, possibly military conflicts. A core problem in cyber diplomacy is the as yet unanswered question of how to deal with borderline situations without established experience-based conflict or war ethics. States can classify a cyber attack as a war attack, in which case the rules of armed war apply. However, there are two key challenges to be dealt with: the attribution dilemma and the disclosure dilemma. The attribution dilemma refers to the difficulty of attributing cyber attacks to specific actors, while the disclosure dilemma concerns the balance between secrecy and the disclosure of information.

Just as in traditional diplomacy, intergovernmental rules of the game and mutual information are extremely important. The European Union (EU) is working within the framework of cyber diplomacy to strengthen its cyber security governance, for

example, in cooperation with the pan-European Police Europol in the European Cybercrime Centre and other EU organisations, such as ENISA (European Network and Information Security Agency) [5]. Cyber dialogues, for example, between the EU and the USA, and multinational formats, such as in the United Nations, are also important components of these efforts.

In addition to building cyber defence capabilities focused on security and defence, cyber diplomacy of Western-oriented states also focuses on the creation of international norms, the protection of data integrity and the promotion of fundamental democratic values, which can serve as a precursor to digital sovereignty. Cyber diplomacy is increasingly proving to be a transformative force in international politics by demonstrating the potential for peacemaking and de-escalation in global conflicts; more than 30 states have already appointed cyber policy envoys, a clear sign of the growing recognition of the importance of this field. In 2015, 25 government experts agreed on behalf of the UN General Assembly that international law should also apply in cyberspace, including the right to defence [6]. With increasing digitalisation, it is becoming more urgent to reach international agreements on rules of engagement in cyberspace in order to minimise the risks of uncontrolled escalation.

For the EU, cyber diplomacy measures include the development of multilateral agreements for trustworthy behaviour in cyberspace, the promotion of cybersecurity and the development of a common foreign and security policy. Specific initiatives include the EU Cybersecurity Act (2019), the EU Cybersecurity Strategy (2020), the joint cyber unit to strengthen defence and law enforcement authorities and the development of multilateral agreements for trustworthy behaviour in cyberspace, as well as measures for a high common level of cybersecurity in the Union, for example, the NIS2 — directive for the cyber and information security of companies and institutions [7].

Preventive measures, such as cyber dialogues and cooperation in the event of conflict, are also an integral part of the EU strategy. Sanctions and export controls, particularly for dual-use technologies, are other important tools in this context.

In the context of cyber diplomacy, it is becoming apparent that the same basic principles apply as in traditional diplomacy, but the novelty and the still limited experience base in this area confront the actors with the challenge of establishing adequate norms and ethical guidelines. These are essential to ensure stability, robustness and resilience in cyberspace. It is recognisable that both state and non-state actors must be integrated into these processes, as both groups play a significant role in cyber diplomacy [8].

Unlike in traditional diplomacy, where private actors and companies generally did not play a prominent active role, their importance in cyber diplomacy is increasing noticeably. This is particularly the case in countries, such as the USA and China, where technology companies hold a dominant position [9]. This development calls for a reassessment of diplomatic interactions and the actors involved.

The emergence of cyber diplomacy as a discipline in its own right reflects the growing recognition that cyberspace is an essential field of international relations. In this context, cyber diplomacy initiatives are aimed at achieving multilateral agreements on cyber norms, responsible behaviour by states and non-state actors in cyberspace and effective global digital governance [10]. The aim is to create an open, free, stable and secure cyberspace that is embedded in international law and based on alliances between like-minded countries, organisations, the private sector, civil society and experts.

Diplomacy plays a key role in establishing cooperation among state and non-state entities within cyberspace. However, navigating diplomatic strategies in this domain is fraught with complexities. The rapid and extensive progress in cyberspace technology blurs the lines between physical and digital community interactions. The emerging cyber domain significantly influences how nations perceive their interests in the contemporary world. This domain has turned into a vulnerable spot for governments attempting to balance threat reduction with the exploitation of arising opportunities. With the expanding prospects for innovation in cyberspace, the likelihood of both competition and potential conflict increases [10].

Cyber diplomacy requires constant development and adaptation due to its novelty and the associated challenges. The involvement of various actors, both governmental and nongovernmental, is essential in order to develop and implement effective and sustainable diplomatic strategies and norms in cyberspace [8].

4. Cyber war vs. conventional war

In contrast to conventional war, which involves physical conflict and the use of material weapons, cyber war takes place in digital cyberspace. The definition of *space* here differs from the traditional, territorial concept of *state space*, which describes the political, legislative and executive borders of a state ([11], p. 55). Although this new form of war can be aimed at destroying or impairing a state's digital infrastructure, it can also be waged virtually, across borders and covertly. A key difference lies in the type of weapons and the areas of impact. While conventional wars cause direct physical damage, the use of digital means can range from influencing public opinion and disrupting critical services to generating false information.

In the modern world, war and cyber war constitute a complex and multi-layered field that poses both traditional and new challenges for the understanding of conflicts and their regulation.

Conventional war, traditionally defined, refers to an armed conflict between states or groups, in which regular armed forces are deployed on land, in the air, at sea or, more recently, in space, in compliance with certain legal and ethical norms. This type of war typically involves territorial disputes, with the sovereignty and territorial borders of states playing a central role. The political scientist Zimmer emphasises how state borders mark the political, legislative and executive limits of sovereignty as a result of the Peace of Westphalia in 1648 [11].

In contrast, cyber warfare is a new form of conflict, in which traditional warfare practices are only applicable to a limited extent. Lancelot points out that there are no set rules for warfare. Challenges, such as the lack of territorial attachment in cyberspace as a *de facto* counter concept to the Peace of Westphalia and the difficulty of clearly attributing attackers to states, undermine traditional concepts of state sovereignty and warfare and offer an undefined risk of escalation [4]. The fact that cyber attacks have the potential to escalate into conventional, even nuclear wars and that the escalation case lies in the assessment of the attacked nation, but lacks recognised rules, is a currently unresolved challenge.

A dynamic that may emerge from this calls for a clearer understanding of the nature of cyberspace in politics and emphasises the need for appropriate regulation or at least a common understanding. While cyberspace can be conceptualised as anarchy without any state norm, rule or ethics, as in the origins of the internet [12] which is still being discussed in some cases today ([13], 780 ff.); however, this anarchy would lead to chaos.

Another current point of discussion is the question of whether cyber warfare can be considered a legitimate form of warfare. What exactly is defined as a cyber weapon also remains controversial. While malicious software code is often considered a cyber weapon, it remains unclear whether code that facilitates communication between states or organisations, but facilitates the spread of malicious software should also be classified as such. It also remains unclear whether the aspect of information warfare can be considered a cyber weapon comparable to conventional weapons. States that are often accused of cyber espionage and cyber attacks, such as Russia, China or North Korea, also rely on public diplomacy in various dimensions, with China having a long tradition here [14]. In the digital context, attempts are also being made to influence public opinion, for example, by utilising social media and sometimes also by using false information. Today, states can do this largely undetected. Modern technologies, such as artificial intelligence and constantly growing access to the (mobile) internet, make it even easier to influence opinions and the public [15]. The promotion of foreign policy interests is, therefore, not new, but represents an increasing challenge and cause for concern as the gaps between cyberspace and physical, territorial space and the proportionality of the use of cyber warfare instruments need to be bridged.

5. Cyber armament or digital sovereignty as a diplomatic means of disarmament

Armament can indeed be used as an instrument of diplomacy, although this is often controversial and seems contradictory; a well-equipped military can serve as a deterrent against potential aggressors and give a state greater leverage in international negotiations, and military strength can be used as leverage in diplomatic negotiations to force concessions from other states, but at the same time, armament can lead to arms races and increased tensions, which increases the risk of conflict. Excessive armament can strain international relations and undermine trust between states in the long term. Diplomacy is often about striking a balance between demonstrating strength and promoting cooperation and peace. Armament is only one aspect of a complex set of international relations. Historical examples, such as the Cold War arms race, show how technological superiority can become an important factor in diplomatic negotiations. However, at least in the nuclear age, this resulted in disarmament due to diplomatic successes (**Figure 1**) [16].

The phase after the Second World War led to a massive build-up of nuclear weapons, particularly in the USA and Russia. Although the first diplomatic and scientific communication formats and platforms to build confidence and reduce military threats were initiated as early as the 1960s (e.g. Pugwash Conferences) and the first treaties to slow down the arms race were concluded, the Cold War armament intensified until it reached its peak in the 1980s. It was only after the collapse of the Soviet Union, 40 years after the start of the arms race, that a global reduction in the number of nuclear warheads could be observed. Other countries such as India, Pakistan and North Korea only entered the arms race in the 1990s.

Armament can be a means to strengthen positions for diplomacy [17]. (Military) superiority in all (military) dimensions weakens the basis for negotiations between opponents. This applies to the military dimensions of land, air, sea and space and therefore also to the cyber dimension [18]. The development of cyber defence and attack capabilities can be seen as a form of modern armament. Such capabilities serve

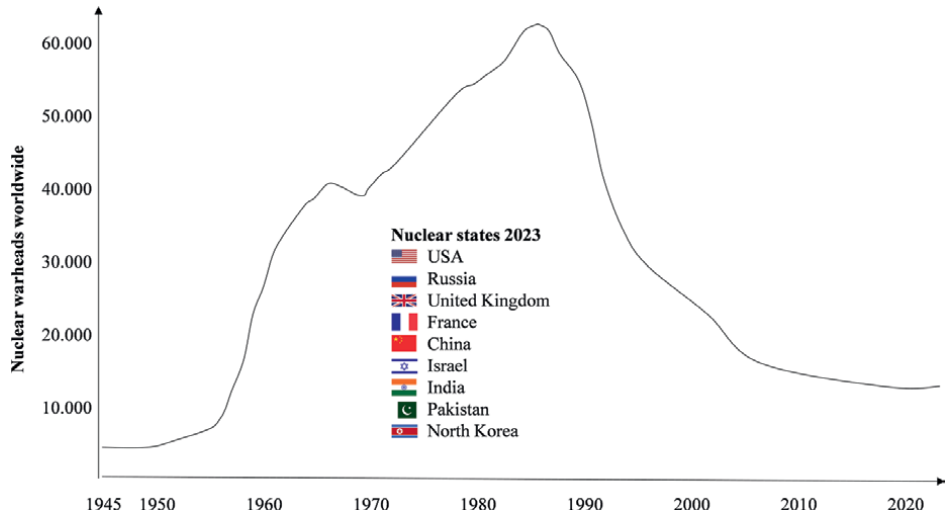

Figure 1.
Disarmament and rearmament of nuclear weapons (own illustration based on [16]).

not only for potential defence but also as a means of strengthening negotiating positions. However, assessing the (necessary) level of armament is far more difficult than in the nuclear armament example outlined above, in which the number of nuclear warheads was analysed.

Presumably, the current cyber threats will also initially lead to armament and then — hopefully, after the emergence of standards and rules — to disarmament. The question of whether this will continue for several decades remains unanswered. The concept of digital sovereignty focuses not only on cyber capabilities but also on the fundamental ability of a state to make strategically autonomous decisions about the information technology it uses and not to make itself dependent on other states.

Capability building is also a key aspect of cyber diplomacy, as the example of Estonia in its Foreign Policy Strategy 2030 shows [19]. Digital capabilities of a digitally sovereign state, its citizens and national companies support the position of a state at the negotiating table with potential conflict partners as the digital defence capability is strengthened. Armament in the sense of strengthening digital sovereignty can, therefore, be described as a 'weapon' in the arsenal of diplomatic instruments.

Experience from nuclear armament should teach us to focus on disarmament and communication instead of armament and isolation [20]. Standardisation aimed at joint disarmament plays a central role here. The EU's cyber diplomacy should focus on the informational self-determination of citizens, the EU's strategic capacity to act in the services of digital sovereignty and European resilience in cyber diplomacy. This includes the harmonisation of IT security legislation at EU level, as well as coordination and procurement in cooperation with international partners.

6. Limits of diplomacy

History teaches that diplomacy has its limits, especially in situations where fundamental interests or values are at stake. In the context of cyber warfare, these limits

become even more unclear as the perpetrators of cyber attacks are often difficult to identify and the attacks are often covert. The extent to which traditional diplomatic approaches need to be adapted in the digital era is being discussed. On the one hand, the same diplomatic practices apply; on the other hand, different countries and organisations are pursuing different approaches in the current discussion about cyber attacks and their regulation. The concept of proportionality plays a central role here. The key question here is 'Which cyber attack is appropriate to respond to with conventional means?' [21]. In the USA, for example, the Department of Defence's Manual on the Law of War regulates the proportionality rules in relation to cyber attacks [22]. This manual serves as a guideline for assessing when and how cyber attacks can be carried out in accordance with the law of war, that is, with conventional weapons. Article 5 of the NATO North Atlantic Treaty states that cyber attacks can trigger a mutual defence situation, which underlines the importance of cyber operations in the context of collective security efforts. In some states, the concept of cyber intervention response or cyber incident detection has been developed to take both defensive and offensive measures in the event of war or for defence in cyberspace [22]. However, these activities are not currently envisaged in peacetime. This concept also serves as a deterrent.

The complexity lies in the fact that there are no generally accepted international rules for the use of cyber attacks or hackbacks. Most states refrain from taking such measures. In the event of a cyber attack, a state is entitled to exercise the right of self-defence in accordance with jus ad bellum, as outlined in the US Department of Defense manual [4, 22]. A prominent example of this is the Stuxnet attack on the SCADA systems of Iranian uranium enrichment facilities, which shows that a cyber attack does not necessarily have to be responded to with a cyber attack [21].

The nature of war and diplomacy in cyberspace can be disorienting and borderless, requiring continuous adaptation and revision of international norms and rules to address the unique challenges of cyberspace. Countries, such as Russia and China, play a central role in cyber diplomacy. Both nations have developed extensive cyber capabilities and use them both defensively and offensively in hashbacks [15]. Their activities in cyberspace have provoked international reactions ranging from diplomatic talks to sanctions [23]. This development highlights how digital sovereignty and cyber capabilities are increasingly becoming key factors in international relations. Some notable cyber attacks discussed in this context include incidents targeting government institutions or the healthcare system in EU states, the influencing of elections in Ukraine and activities just prior to Russia's military attack against Ukraine. Another prominent example is Russia's alleged influence on the US elections in 2016, in which cyber operations are said to have played a central role in influencing the election.

These incidents illustrate the diverse applications of cyber operations, ranging from targeted attacks on critical infrastructure to influencing political processes. They not only highlight the vulnerability of democratic processes to cyber attacks but also underline the need for robust cyber defence and diplomacy [24].

Also, noteworthy in this context is the bilateral declaration of a new strategic partnership between Russia and China in 2016, which includes cooperation in the field of information technology and communications (ICT). Both countries expressed their concern that ICT could be used to interfere in the internal affairs of other states. This agreement can be interpreted as an attempt at compartmentalisation and axis building, as Bendiek notes [6]. It reflects the increasing importance of cyber operations in

international politics and the endeavours of some states to protect and promote their own interests and sovereignty in the digital space.

China's territorially delimited institutionalism, for example, produces digital technologies largely independently through strong regulation and isolation, following the desire for cyber sovereignty. This is an expression of the Chinese Communist Party's concept to exercise state control over private-sector industries and technologies and to enforce the interests of the nation-state's cybersecurity strategy, which is in stark contrast to multi-stakeholder management ([25], pp. 107-131). China is pursuing a state-institutionalised, autarky-oriented and digital-policy concept to strengthen its sovereignty. Since 1972, technology transfer from abroad has been systematically ensured; regulation, state control and a five-year plan in the 30 most important policy fields have been the focus of government action; A total of 12 possibilities of legal technology transfer, 12 of extra-legal technology transfer and eight of illegal technology transfer have been described [15], indicating that China will further strengthen its digital dominance and independence ([26], p. 169).

It is, therefore, foreseeable that a new world order will also emerge in cyberspace. It is still unclear — as the current positioning discussions surrounding Russia's war of aggression against Ukraine show — how states such as India or the BRICS countries will position themselves [9]. However, it is clear that the EU states must strengthen themselves against possible new axes in the cyber world in order to maximise the limits of cyber diplomacy and avoid possible escalations.

7. Cyber resilience

The cyber resilience and cyber security of countries is measured by various indices, such as the global cybersecurity index (GIS), the index of cybersecurity (ICS) and the national cybersecurity index (NCSI) [27, 28]. It describes the ability of a country to protect itself against cyber attacks, respond to them and recover from their effects. The indices make it possible to compare the cyber competences and resilience of different countries.

Cyber security is an essential component of digital sovereignty as increasing cyber attacks can threaten the sovereignty of states. Many examples of government and industrial organisations, especially critical infrastructure such as banks, energy suppliers and hospitals, that have been blackmailed or compromised by cyber attacks illustrate the impact of cyber attacks on the global economy [29]. Especially since Russia's war against Ukraine, the number of cyber attacks has increased. Therefore, cyber security has a direct and increasing influence on the sovereignty of states and is conceptually linked to it [30].

The NCSI, which has been compiled by the e-Governance Academy in Estonia since 2018, measures the effectiveness of 173 countries in defending themselves against cyber attacks such as denial of service attacks or data integrity breaches, using 46 indicators from predominantly administrative areas. According to the NCSI, state-level capabilities include, for example, the ability to regulate cyber attacks, cooperation, security policy and crisis management. Analysis of the ranking shows that many American, Asian and European states, as well as Australia, have a relatively high cyber security ranking. Many of these states are also autocratic states, for which cyber defence is also an essential attribute of digital sovereignty in the sense of isolation and the protection of autocratic structures [27]. Therefore, it can be said that cyber

resilience is an essential attribute of digital sovereignty for both democratic states, including all EU member states, and non-democratic states.

The importance of cyber resilience has emerged as a key aspect of national security strategies. This capability can also serve as a deterrent to prevent potential attackers from conducting offensive cyber operations.

Cyber attacks often target not only critical infrastructures such as water and electricity supply, transport, retail and healthcare but also universities and government institutions. The intention behind such attacks can vary from state-motivated espionage and the endeavour to weaken the structures of a state to economically motivated attacks by trolls who, for example, encrypt computers using Trojans and extort ransom money.

Countries take different approaches to strengthening their cyber resilience. The US has developed a number of strategies and laws, including the National Strategy for Cyberspace (2002), the National Plan to Secure Critical Infrastructure (2006) and the Comprehensive National Cybersecurity Strategy (2008) [5]. The Cyber Diplomacy Act (2021) aims to strengthen US global leadership in cybersecurity.

Australia has significantly strengthened its cyber defence capabilities in recent years with a focus on strengthening the resilience of its critical infrastructure and promoting cyber security literacy within the population [10].

In Europe, the focus is on developing cyber defence technologies, strengthening digital markets and infrastructures and promoting digital sovereignty. The European Commission emphasises the importance of upgrading and developing resilience to cyber attacks [18].

China has implemented comprehensive national cyber security strategies that focus on the protection of critical infrastructure and the development of advanced cyber defence capabilities in terms of compartmentalisation indicating that it will further strengthen its digital dominance and independence [26].

Cyber diplomacy includes the development of cyber defence techniques, the promotion of growth and resilience of digital infrastructures and markets, as well as the arming and strengthening of relevant organisations against cyber attacks.

The global perspectives on cyber resilience are diverse and complex. Various institutions contribute to the development and implementation of cyber security strategies [5].

To be taken seriously in the cyber arena, Western states must also strengthen their cyber resilience through deterrence and armament in order to step out of the role of the underdog. This requires a balanced combination of technological development, strategic planning and international cooperation. Educating the population, robust IT systems and resilient structures, including backups and manual procedures, are essential.

8. Digitalisation and digital sovereignty

This section differentiates between digitalisation and digital sovereignty. It also analyses how different geopolitical actors — including China, the USA, Europe, Africa and the BRICS states — define and implement the concept of digital sovereignty. It analyses how these different approaches influence international politics and diplomacy.

Digital sovereignty describes the ability of a state or region to control and manage digital infrastructure, data and communication with a relevant degree of autonomy (**Figure 2**).

The approach should not be confused with digital self-sufficiency or autarky in the form of isolation as demonstrated by China, for example. Rather, digital sovereignty as

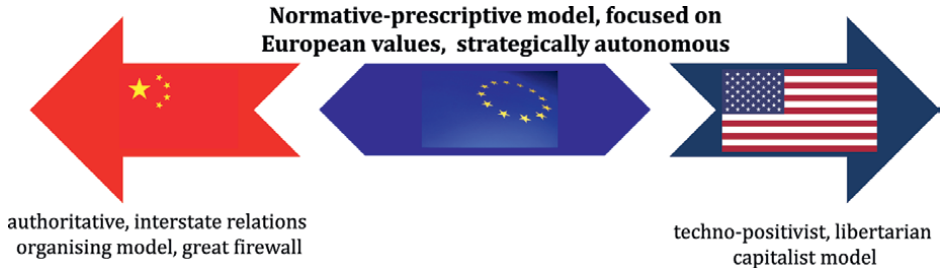

Figure 2.
Interpretations of digital sovereignty based on [31].

autonomy describes a form of independence in technology selection and thus robustness and resilience. This ability becomes particularly relevant when the sovereignty of a state, that is, the ability to make independent decisions in matters of internal and external sovereignty, is potentially jeopardised by dependencies or the influence of third parties — especially states or other institutions with divergent understandings of political systems. This includes the development of its own technologies and standards, the protection of data and the establishment of a robust digital economy. The approaches taken by different states or regions to strengthen digital sovereignty diverge significantly.

China practices a policy of strict control and censorship of the internet, known as the 'Great Firewall'. This approach is aimed at ensuring national security and controlling the spread of content deemed harmful to social stability or the interests of the ruling party. China also encourages the development of indigenous technologies and digital platforms to reduce dependence on foreign technologies, thereby pursuing an autarchic and autocratic approach [26].

The United States pursues a neo-liberal and market-orientated approach to digital sovereignty. The US government generally supports the development and growth of technology companies, but intervenes comparatively little in their operations. Despite a fundamentally techno-positivist, liberal and capitalist system, there are growing concerns about privacy, data security and the power of large technology companies, leading to calls for stricter regulation [26].

The countries of Europe, particularly those within the European Union (EU), have demonstrated a strong commitment to the principles of data protection and security. This commitment is evidenced by the introduction of robust data protection laws, such as the general data protection regulation (GDPR). European policies, regarding digital sovereignty, are primarily focused on multiple key aspects: protecting the privacy rights of individual citizens, promoting transparency in data handling and usage and ensuring that there is a fair and level competitive environment for all companies operating within this space [32]. These approaches reflect a broader European vision of balancing technological advancement with fundamental rights and equitable business practices. A normative-prescriptive model is being pursued that is in line with the liberal and democratic values of the EU member states. In the context of digital sovereignty, there is often talk of 'strategic autonomy' [31].

African countries are still in the phase of expanding their digital infrastructure. The focus is often on expanding access to digital services and developing local digital markets. Some countries have launched initiatives to promote digital education and support local technology start-ups [33].

The BRICS group of emerging economies (Brazil, Russia, India, China, South Africa) have different approaches to digital sovereignty. While Russia, such as China,

pursues a highly controlled and autocratic approach, countries, such as India and Brazil, practise more liberal policies that support the free flow of information and the development of technology companies [34].

Australia is pursuing its own approach to digital sovereignty, which integrates elements of data protection, security and economic development. Various measures have been implemented to ensure the security and protection of digital data. This includes legislation that defines how companies and organisations must handle personal data [35]. There is an increasing focus on cyber security to protect state and private digital systems from threats. Despite the focus on national sovereignty, Australia is also engaged internationally to help shape global standards and norms for the internet and digital technologies, both through bilateral agreements and participation in multilateral forums [10].

The approaches outlined above reflect the divergent political, economic, social and cultural realities of each state or region. Digital sovereignty remains a complex and sometimes contradictory concept, influenced by global developments and a constantly changing technological landscape, and is increasingly becoming an instrument of power politics. However, the concept can still largely be described in qualitative terms.

The measurability of digital sovereignty is still in its infancy. Initial approaches to creating a digital sovereignty index (DSI) for states are at an early stage [36]. Although there are numerous concepts for assessing state sovereignty, such as the World Governance Index [37] or the Barnett Index [38], as well as indices for assessing the digitalisation of states [39]. A recognised index on digital sovereignty, which converges the concepts of sovereignty and digitalisation and their measurability, is currently being developed; a DSI consisting of 30 parameters to assess sovereignty in the context of European values, the ability to develop key technologies and technological independence. The collection of secondary data and suitable aggregation results in an index value per country that can be ranked [40].

9. Cyber resilience and digital sovereignty: two divergent concepts?

Cyber resilience has become a central aspect of national security strategies [18, 41]. Digital sovereignty, on the other hand, is a concept for defining and evaluating the capabilities of states to reduce one-sided technological dependencies and thereby protect state institutions and critical infrastructures [31].

Both concepts could correlate in the sense that a digitally sovereign state also has a high level of cyber resilience and vice versa. However, this is not the case. Countries that are exposed to a high cyber threat (e.g. Russia, China, North Korea) have high cyber resilience scores. The NCSI uses the years 2016-2023 as a basis for assessment and ranks Belgium, Lithuania, Estonia, Czech Republic, Germany, Romania, Greece, Portugal, United Kingdom and Spain in the top 10 [28].

After Russia's war of aggression against Ukraine, the ranking will probably change in 2024 (Poland, Estonia, Ukraine, Latvia, United Kingdom, Albania, Moldova, Georgia, China, Saudi Arabia), but the TOP NCSI countries are neither particularly highly digitalised nor do they stand out due to their high democracy scores if the definition of digital sovereignty used in the previous section is used. From this, it can be hypothesised that the European understanding of digital sovereignty so a normative-prescriptive model does not directly contribute positively to cyber resilience as it is formulated rather defensively.

The two previously mentioned indices, the digital sovereignty index (DSI) (DSI) and the national cyber security index (NCSI), are used to confirm the hypothesis. The DSI measures parameters relating to state sovereignty, key technologies and technological sovereignty, while the NCSI measures cyber security policy, a state's contribution to global cyber security, education and professional development [27, 40]. The hypothesis to be rejected is, therefore, as follows: The higher the DSI/NCSI rank, the higher the digital sovereignty/cyber resilience rank of a state (**Figure 3**).

The correlation between the EU countries shown here and Australia, China, Russia and the USA is weak. The coefficient of determination is only 0.5%, that is, there is no significant linear correlation between the NCSI and the DSI. The Pearson and Spearman coefficients of approximately 0.071 and 0.048 also show very weak positive correlations. Those countries with a high NCSI ranking, such as Belgium, Estonia, Latvia, the Czech Republic or Germany, are in the midfield of the digital sovereignty index [13, 16, 23, 33, 30]. In contrast, the USA, the leading country in the DSI, is ranked 42nd in the NCSI, while Russia and China are in the middle of the field in both indices, although both countries play a major role in cyber attacks.

In this respect, the two concepts cannot be contradictory or at least not interdependent. In other words, a state that places a high focus on cyber resilience does not necessarily have to have well-developed digital sovereignty capabilities, and conversely, a digitally sovereign state does not necessarily have to have a high level of cyber resilience. One possible reason for this — using the example of the USA or China — may be that cyber resilience, cyber defence and cyber war in the dimensions of land, sea, air, space and cyber only serve one domain and other economic or political aspects play a greater role.

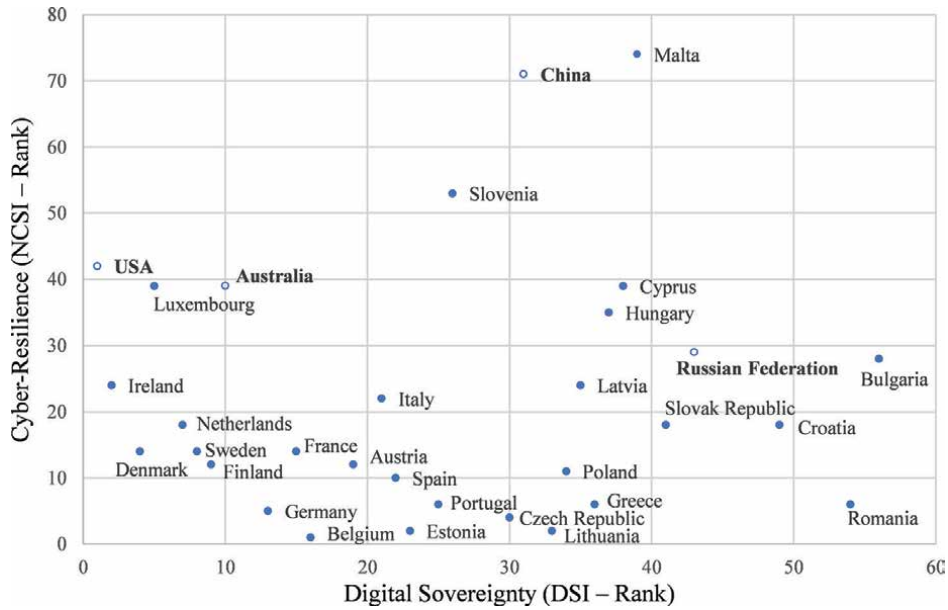

Figure 3.
DSI/NCSI rank correlation, EU and USA, China, Russia, Australia.

10. Cyber resilience and digital sovereignty as a diplomatic tool

The exploration of digital sovereignty and cyber resilience as diplomatic tools, as in the previous sections, necessitates an in-depth examination of their multifaceted functions, far-reaching effects and strategic significance within the landscape of international relations. Both concepts, while distinct in their focuses, converge to shape the contours of contemporary diplomacy, offering nations a means to assert their autonomy, safeguard their interests and foster cooperation in an increasingly digitised world. At its core, digital sovereignty embodies a state's capacity to assert control and autonomy over its digital ecosystem, encompassing its infrastructure, data management practices and technological advancements. This pivotal concept empowers nations to chart their own course in the digital realm free from external coercion or influence [36, 42]. By exercising sovereignty over their digital domains, states can mitigate vulnerabilities, assert their diplomatic agency and navigate the complexities of global affairs with confidence. Moreover, robust digital sovereignty not only bolsters a nation's negotiating prowess but also fosters trust and collaboration among peers, laying the groundwork for the establishment of international norms and rules that promote responsible behaviour in cyberspace and mitigate the risk of conflicts and wars.

Similarly, cyber resilience emerges as a cornerstone of modern diplomacy, epitomising a state's ability to withstand, respond to and recover from cyber threats. A nation fortified with high levels of cyber resilience is better equipped to defend against cyber attacks, mitigate their impact and deter potential adversaries from engaging in hostile activities [27]. By investing in robust cyber defence mechanisms, cultivating a skilled workforce and fostering international cooperation, states can bolster their cyber resilience capabilities, fortify national security and uphold stability within their borders. Furthermore, collaborative efforts in cyber resilience serve as conduits for building trust, sharing information and fostering mutual understanding among nations, thereby strengthening diplomatic relations and averting potential conflicts.

In essence, digital sovereignty and cyber resilience converge to shape the fabric of modern diplomacy, offering a pathway towards a stable, secure and cooperative international order. By prioritising these concepts, states not only safeguard their own security and interests but also contribute to the broader goal of global peace and stability. As nations navigate the complexities of an interconnected world, the continued advancement of digital sovereignty and cyber resilience emerges as a critical imperative, ensuring that diplomacy remains effective in addressing the evolving challenges of the digital age and fostering a more harmonious and prosperous global community.

11. Conclusions

'In an era defined by the omnipresence of digital technologies and interconnected networks, the concepts of digital sovereignty' [42, 43] and cyber resilience have evolved into indispensable cornerstones of contemporary diplomacy [38]. As nations grapple with the complexities of an increasingly digitised world, these principles have emerged as essential tools for safeguarding national interests, 'preserving global stability and mitigating the risks' posed by cyber threats and conflicts [44].

At its core, digital sovereignty encapsulates a state's ability to assert control and autonomy over its digital infrastructure, data governance and cyber policies [43]. It embodies the notion of self-determination in the digital realm, enabling nations to make independent and strategic decisions that safeguard their sovereignty and protect against external interference. In an age where cyberspace knows no borders, digital sovereignty serves as a bulwark against cyber espionage, data breaches and other forms of digital manipulation, empowering nations to uphold their values and interests in an interconnected world [13].

Complementing digital sovereignty is the concept of cyber resilience, which encompasses a state's capacity to withstand, adapt to and recover from cyber threats and attacks. Unlike traditional notions of security, cyber resilience emphasises agility, adaptability and proactive risk management in the face of evolving cyber threats [27]. It involves not only the deployment of robust cybersecurity measures but also the cultivation of a resilient cyber culture that prioritises continuous learning, innovation and collaboration across sectors. By fostering a culture of resilience, nations can minimise the impact of cyber incidents, mitigate potential disruptions to critical infrastructure and maintain trust and confidence in the digital economy and society.

While digital sovereignty and cyber resilience can be discussed as separate concepts, their interplay is essential in shaping effective cybersecurity strategies and diplomatic engagements in the digital age. They could form a symbiotic relationship that enables nations to navigate the complexities of cyberspace with confidence and purpose. Digital sovereignty provides the foundation for establishing clear norms, rules and principles governing state behaviour in cyberspace, while cyber resilience ensures the resilience and robustness of digital infrastructure and systems, thereby reinforcing national sovereignty and security in an interconnected world.

Furthermore, the convergence of digital sovereignty and cyber resilience offers opportunities for collaborative diplomacy and multilateral cooperation in addressing shared cyber challenges. By leveraging their collective expertise, resources and capabilities, nations can enhance cyber resilience at the regional and global levels, promote information sharing and capacity building and develop norms and standards that promote a safe, secure and open cyberspace for all. Through diplomatic channels such as bilateral dialogues, international conferences and cyber diplomacy forums, states can engage in constructive discussions on cybersecurity issues, build trust and confidence among stakeholders and forge consensus on key policy priorities and initiatives.

In conclusion, digital sovereignty and cyber resilience are integral components of modern diplomacy, offering nations the means to navigate the opportunities and challenges of an increasingly digitised world. By embracing these principles and fostering international cooperation, nations can strengthen their cybersecurity posture, protect their national interests and promote peace, stability and prosperity in the digital age. As cyberspace continues to evolve and shape the global landscape, the imperative for robust cybersecurity strategies and diplomatic engagements will only grow, making digital sovereignty and cyber resilience essential pillars of twenty-first century diplomacy.

Conflict of interest

The author declares no conflict of interest.

Author details

Martin Kaloudis
Mendel University in Brno, Czech Republic

*Address all correspondence to: martin@kaloudis.de

IntechOpen

References

[1] Arnold H. Frieden und diplomatie. In: Gießmann H-J, Rinke B, editors. Handbuch Frieden. 1st ed. Wiesbaden: VS Verl. für Sozialwiss; 2011. pp. 294-309

[2] Blessing J. The global spread of cyber forces, 2000-2018. In: Jančárková T, Lindström L, Visky G, Zotz P, editors. 2021 13th International Conference on Cyber Conflict: Going Viral: CyCon. Tallinn, Estonia: IEEE; 2021. pp. 233-255

[3] Hall I. Systems of states. In: Hall I, Wight M, editors. Palgrave Macmillan History of International Thought Series, The International Thought of Martin Wight. 1st ed. Basingstoke: Palgrave Macmillan; 2006. pp. 87-110

[4] Lancelot JF. Cyber-diplomacy: Cyberwarfare and the rules of engagement. Journal of Cyber Security Technology. 2020;**4**(4):240-254. DOI: 10.1080/23742917.2020.1798155

[5] Cirnu C-E, Rotuna C-I, Vasiloiu I-C. Comparative Analysis on Cyber Diplomacy in EU and US. ROCYS. 2023;**5**(1):77-86. DOI: 10.54851/v5i1y202307

[6] Bendiek A. The EU as a Force for Peace in International Cyber Diplomacy. Stiftung Wissenschaft und Politik -SWP-Deutsches Institut für Internationale Politik und Sicherheit, Berlin. 2018

[7] Vandezande N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review. 2024;**52**:105890. DOI: 10.1016/j.clsr.2023.105890

[8] DeNardis L, Raymond M. Thinking clearly about multistakeholder internet governance. (November 14, 2013). GigaNet: Global Internet Governance Academic Network, Annual Symposium. 2013. Available from: https://ssrn.com/abstract=2354377

[9] Couture S, Toupin S. What does the notion of "sovereignty" mean when referring to the digital? New Media and Society. 2019;**21**(10):2305-2322. DOI: 10.1177/1461444819865984

[10] Manantan MBF. Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. Australian Journal of International Affairs. 2021;**75**(4):432-459. DOI: 10.1080/10357718.2021.1926423

[11] Zimmer M. Moderne, Staat und Internationale Politik. 1st ed. Wiesbaden: Verlag für Sozialwissenschaften; 2008 [Online]. Available from: http://gbv.eblib.com/patron/FullRecord.aspx?p=752384

[12] Barlow JP. A declaration of the independence of cyberspace [Online]. Available from: https://www.eff.org/cyberspace-independence

[13] Mueller ML. Against Sovereignty in Cyberspace. International Studies Review. 2020;**22**(4):779-801. DOI: 10.1093/isr/viz044

[14] Burt S. China's use of public diplomacy in the United States: From World War II to the twenty-first century. In: Turcanu-Carutiu D, editor. Heritage. London, UK: IntechOpen; 2020

[15] Hannas WC, Tatlow DK. China's Quest for Foreign Technology: Beyond Espionage. London, New York: Routledge; 2021

[16] Kristensen HM, Norris RS. Global nuclear weapons inventories, 1945-2013. Bulletin of the Atomic Scientists. 2013;**69**(5):75-81. DOI: 10.1177/0096340213501363

[17] Sumantri TB, Achmad NI, Kumalasari D. The history of nuclear armament technology as an introduction to understand the dynamic of international society. In: Rochmat S, Aman A, Zulkarnain Z, Kumalasari D, Agustinova DE, editors. Advances in Social Science, Education and Humanities Research, Proceedings of the Annual Conference on Research, Educational Implementation, Social Studies and History (AREISSH 2021). 1st ed. Vol. 681. Paris: Atlantis Press SARL; Imprint Atlantis Press; 2023. pp. 216-224

[18] Dawda S. Exploring National Cyber Security Strategies. Occasional Paper. 2021

[19] Barrinha A. Virtual Neighbors: Russia and the EU in Cyberspace. Insight Turkey. 2018;**20**(3):29-42 [Online]. Available from: http://www.jstor.org/stable/26469842

[20] Bendiek A, Kettemann MC, Stiftung Wissenschaft Und Politik. EU-Strategie zur Cybersicherheit (in deu). Berlin: Deutsches Institut für Internationale Politk und Sicherheit; 1611- 63642021. p. 8. DOI: 10.18449/2021A12 [Accessed: Dec 2023]

[21] Hjorthen FD, Pattison J. Proportionality in cyberwar and just war theory. Ethics & Global Politics. 2023;**16**(1):1-24. DOI: 10.1080/16544951.2023.2179244

[22] Preston SW. Department of Defense Law of War Manual. Washington; 2023 [Online]. Available: https://apps.dtic.mil/sti/citations/trecms/ad1207225

[23] Kukkola J, Ristolainen M, Nikkarila J-P. GAME PLAYER Facing the Structural Transformation of Cyberspace. Vol. 11. Kista, Finnland: Finnish Defence Research Agency Publications; 2019

[24] Lee J. Review of the Mueller Report. Journal of Business Ethics. 2020;**163**(1):167-172. DOI: 10.1007/s10551-019-04357-8

[25] Creemers R. Governing Cyberspace: Behavior, Power, and diplomacy, China's Conception of Cyber Sovereignty. Lanham: Rowman & Littlefield; 2020

[26] Holtmann D. Potsdamer Beiträge zur Sozialforschung: Die Performanz von Politik, Wirtschaft und Gesellschaft für 43 Länder und six Wohlfahrtsregime. Potsdam: Wirtschafts- und Sozialwissenschaftliche Fakultät/Sozialwissenschaften; 2018 [Online]. Available from: https://www.ssoar.info/ssoar/bitstream/handle/document/58258/?sequence=1 [Accessed: Apr. 22, 2022]

[27] Kravets V. Comparative Analysis of the Cybersecurity Indices and Their Applications. TACS. 2019;**1**(1). DOI: 10.20535/tacs.2664-29132019.1.169090

[28] e-Governance Academy. NCSI - national cyber security index [Online]. Available from: https://ncsi.ega.ee/ncsi-index/

[29] Balbaa ME, Eshov MP, Ismailova N. The Impacts of Russian Ukrainian War on the Global Economy in the frame of digital banking networks and cyber attacks. In: Proceedings of the Sixth International Conference on Future Networks & Distributed Systems. New York, NY, USA; 2022

[30] Madiega TA. Digital sovereignty for Europe. European Parliamentary Research Service. 2020 [Online]. Available from: https://policycommons.net/artifacts/1336893/digital-sovereignty-for-europe/

[31] Pohle J, Thiel T. 2.3.2 Digitale Souveränität. In: Piallat C, editor.

Digitale Gesellschaft, Band 36, Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt. Bielefeld: Transcript; 2021. pp. 319-340

[32] de Carvalho D, Leonor S. Key GDPR elements in adequacy findings of countries that have ratified convention 108. European Data Protection Law Review. 2019;**5**(1):54-64. DOI: 10.21552/edpl/2019/1/9

[33] Worldbank. Accelerating Digital Transformation in West Africa. Available from: https://www.worldbank.org/en/news/press-release/2023/12/01/accelerating-digital-transformation-in-west-africa [Accessed: Dec. 01, 2023]

[34] Polatin-Reuben D, Wright J. An internet with {BRICS} characteristics: Data sovereignty and the balkanisation of the internet. In: Fourth USENIX Workshop on Free and Open Communications on the Internet (FOCI 14). Vol. 2014. 2014 [Online]. Available: https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben

[35] Mitchell AD, Samlidis T. Cloud services and government digital sovereignty in Australia and beyond. International Journal of Law and Information Technology. 2022;**29**(4):364-394. DOI: 10.1093/ijlit/eaac003

[36] Kaloudis M. Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan? New Global Studies. 2021;**16**(3) 275-299. DOI: 10.1515/ngs-2021-0015

[37] Arndt C. The Politics of Governance Ratings. International Public Management Journal. 2008;**11**(3):275-297. DOI: 10.1080/10967490802301278

[38] Barnett MA. Quantifying sovereignty: A new way to examine an essential concept [Online]. Available from: https://dash.harvard.edu/handle/1/33825923

[39] European Commission. Digital economy and society index (DESI) 2022. Thematic Chapters. 2022

[40] Kaloudis M. From Quality to Quantity: How Can Digital Sovereignty be Parsed into Measurable Components? European Journal of Business Science and Technology. 2022;**2022**(2):172-189. DOI: 10.11118/ejobsat.2022.011

[41] World Economic Forum. The US has announced its National Cybersecurity Strategy: Here's what you need to know. 2023. Available from: https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/#:~:text=URL%3A%20https%3A%2F%2Fwww.weforum.org%2Fagenda%2F2023%2F03%2Fus

[42] Pohle J. Digitale Souveränität. In: Klenk T, Nullmeier F, Wewer G, editors. Springer eBook Collection, Handbuch Digitalisierung in Staat und Verwaltung. Wiesbaden: Springer VS; 2020. pp. 1-13

[43] Pohle J, Thiel T. Digital sovereignty. Internet Policy Review. 2020;**9**(4). DOI: 10.14763/2020.4.1532

[44] Guo X, Chmutova I, Kryvobok K, Lozova T, Kramskyi S. The race for global leadership and its risks for world instability: Technologies of controlling and mitigation. RJAH. 2024;**5**(1). DOI: 10.58256/5wzf9y48

Chapter 3

The Front End of Innovation in Defense: A Comprehensive Literature Review

Romullo Girardi, Juraci Ferreira Galdino and Paulo César Pellanda

Abstract

Innovation management, a multifaceted organizational process encompassing opportunities and ideas from inception to implementation, demands a systematic approach, particularly in the critical initial phase known as the Front End of Innovation (FEI). This pivotal phase significantly influences the entire innovation management chain. Despite its recognized importance, FEI in the defense sector has yet to be systematically addressed in the academic literature. Recognizing the vital role of FEI in the defense sector, this study addresses this deficiency through a systematic review, scrutinizing 24 documents from the scientific literature (Scopus and Web of Science databases) and gray literature (government defense documents). This research systematically maps key activities identified in seminal FEI models. These activities include the identification and analysis of opportunities; generation, enrichment, and screening of ideas; product concept definition; and consideration of influencing factors. Concurrently, this work aligns defense practices with established innovation models and provides valuable insights for optimizing the management dynamics of the military innovation process. Through this systematic inquiry, this study contributes to a nuanced understanding of the FEI in the defense sector, offering practical implications for enhancing defense innovation development.

Keywords: innovation, front end of innovation, defense, military, literature review

1. Introduction

Innovation management, a complex and broad organizational process covering the entire spectrum, from identifying new opportunities and ideas to their practical implementation, poses significant challenges for managers across all organizational levels [1].

Notably, innovation seldom fails due to a lack of creativity; instead, it is the absence of discipline that plays a pivotal role in innovation failures [2]. From this perspective, Boeddrich [3] contends that systematic and structured procedures in the early phase, known as the Front End of Innovation (FEI), are imperative to avert adverse effects throughout the innovation management chain.

Multiple researchers emphasize that enhancing FEI activities contributes positively to organizational outcomes, bolstering the likelihood of successful innovation development [3–9]. Yet, the successful adoption of a FEI model requires considering some factors like organizational size and culture, as well as decision-making styles [10, 11].

Despite the increasing attention to FEI as a complex and multidisciplinary field [12], the defense context of FEI has not been sufficiently addressed in the academic literature, a gap this study endeavors to address. Therefore, this research aims to unravel the dynamics of FEI in the military sector through a systematic literature review, focusing on the research question: *How can the current literature on the early phase of the innovation process in defense be mapped within seminal FEI models?*

This question is pertinent given the Armed Forces' distinct organizational culture, demanding innovation to sustain high-tech operational capabilities and mainly requiring innovations capable of inducing technological surprise in the theater of operations. Aligning defense practices with established models in innovation literature can furnish invaluable insights for improving the management dynamics of the military's initial innovation phase. Moreover, by reviewing approaches used by different countries, the study recognizes that the suitability and significance of FEI management practices can differ across national defense contexts. It emphasizes how cultural and procedural nuances impact the development and adoption of new technologies in military settings.

Structured around the research question, this paper is organized as follows: Section 2 provides a theoretical foundation on FEI, seminal FEI models, and defense peculiarities. Section 3 outlines the research methodology. Section 4 delineates the mapping of the FEI in the defense sector within seminal FEI models. Section 5 discusses salient aspects identified throughout the study. Finally, Section 6 highlights the concluding remarks, outlining directions for future research.

2. Theoretical foundation

Before exploring the current literature on the early stage of the innovation process in defense, it is essential to understand the foundational topics involved: the FEI concept, the seminal FEI models, and the unique aspects of the military sector.

2.1 Front end of innovation (FEI)

The Fuzzy Front End (FFE) refers to the earliest stage in the New Product Development (NPD) process. This term was popularized by Smith and Reinertsen [13], as pointed out by Khurana and Rosenthal [10].

In 2002, Koen et al. [14] proposed the term Front End of Innovation (FEI), considering that the adjective "fuzzy" is "mysterious, lacks accountability, and cannot be critically evaluated" ([14], p. 30). The new term dissociated the idea that the initial phase of the innovation process was nebulous and uncontrollable. In this approach, the FEI is described as "those activities that come before the formal and well-structured NPD process" ([14], p. 30).

Figure 1 illustrates the breakdown of the product innovation management process into three phases: FEI, NPD, and implementation (the commercialization of the product in the market). The circular shape of the FEI suggests that ideas should

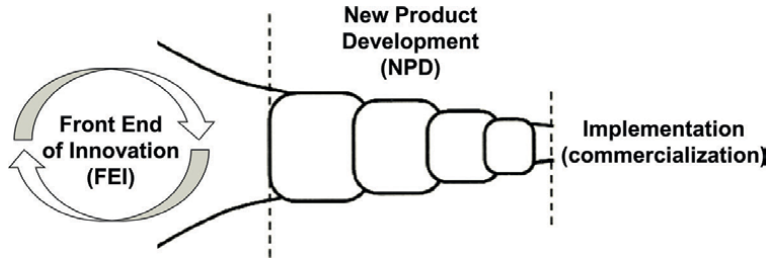

Figure 1.
Breakdown of the product innovation management process. Source: Adapted from Koen et al. [14, 15].

flow and iterate until the formal definition of products is developed. In contrast, the NPD phase is depicted as a series of sequential, well-structured, and chronologically ordered steps [14, 15].

The FEI emerges as a crucial driver of positive outcomes for new products and, consequently, the overall success of the business [16]. Markham [6] underscores the profound impact of early-phase activities on product performance, emphasizing that the success of the front end stands as the strongest independent predictor of all NPD performance variables.

Selecting an appropriate FEI model requires careful consideration of various factors, including organizational size and culture, as well as decision-making style [10, 11]. As a response to these diverse organizational needs, numerous FEI models have been developed over time, offering distinct approaches to navigate their complexities, as detailed in the next section.

2.2 Seminal FEI models

In an integrative literature review, Pereira et al. [12] found that 26% of articles related to FEI contributed in terms of frameworks, models, processes, tools, and methodologies, exemplifying endeavors to structure the early phase of the innovation process in specific contexts.

While recent contributions are significant, seminal works have produced models that served as reference points for structuring the FEI. **Table 1** provides an overview of the four seminal models identified by Pereira et al. [12, 20].

After providing an overview of the seminal FEI models, it is essential to delve into the main elements of their structures. The stage-gate model, proposed by Cooper [17, 18], offers a systematic approach to the FEI through its first three stages/gates, as depicted in **Figure 2**. The process unfolds in distinct phases as follows:

- *Stage 0 (Discovery)*: In this inaugural stage, the organization actively generates ideas for new products.

- *Gate 1 (Idea screen)*: Ideas undergo a concise evaluation based on strategic, feasibility, and market criteria. Financial considerations are deferred at this point. Accepted ideas proceed to the next phase.

- *Stage 1 (Scoping)*: The accepted idea transitions into a project, initiating a dual evaluation process:

References	Model	Overview
Cooper [17, 18]	Stage-Gate	Proposes a system with well-defined stages to launch new products into the market. The early stages represent the front end of innovation and make use of control gates.
Khurana and Rosenthal [10, 11]	Three Phase Front End	Presents an approach that connects business and product strategy with specific product-related decisions.
Koen et al. [14, 15]	New Concept Development	Provides methods, tools, and techniques suitable for managing the front end of innovation. Moreover, the authors seek a common vision and terminology for the FEI.
Reid and De Brentani [19]	The Fuzzy Front End of New Product Development for Discontinuous Innovations	Details an approach focusing on disruptive innovation, proposing a structure based on a reverse flow of information (from the outside world into the organization).

Source: Adapted from Pereira et al. [12, 20].

Table 1.
Seminal FEI models.

  - *Market evaluation*: Involves research, user contact, and conceptual testing to determine market size and acceptance.
  - *Technical evaluation*: Encompasses feasibility, costs, and development timelines.

- *Gate 2 (Second screen)*: Comprehensive information from market and technical evaluations prompts a reassessment of the project's viability. If approved, the project advances to the next stage.
- *Stage 2 (Build business case)*: Positioned just before product development, this stage involves:
  - Assessing the project's attractiveness.
  - Defining clear objectives.
  - Conducting market, technical, operational, and financial evaluations.
- *Gate 3 (Development)*: A pivotal decision point where the organization determines resource allocation for project development [17, 18].

The Three Phase Front End model, proposed by Khurana and Rosenthal [10, 11], organizes the FEI into three distinct phases, as depicted in **Figure 3**.

- *Pre-Phase Zero*: This initial phase concentrates on the continuous identification of opportunities within the organization. It involves generating ideas and conducting technological and market analyzes. When a promising opportunity is identified, it triggers the transition to Phase Zero. The authors emphasize that this phase should occur continuously within the organization.

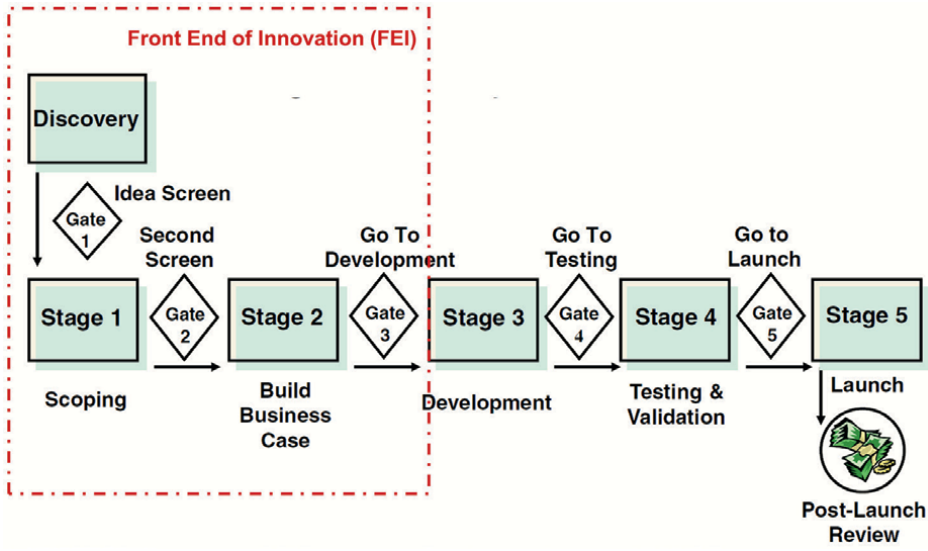

Figure 2.
The FEI within the stage-gate model. Source: Adapted from Cooper [17].

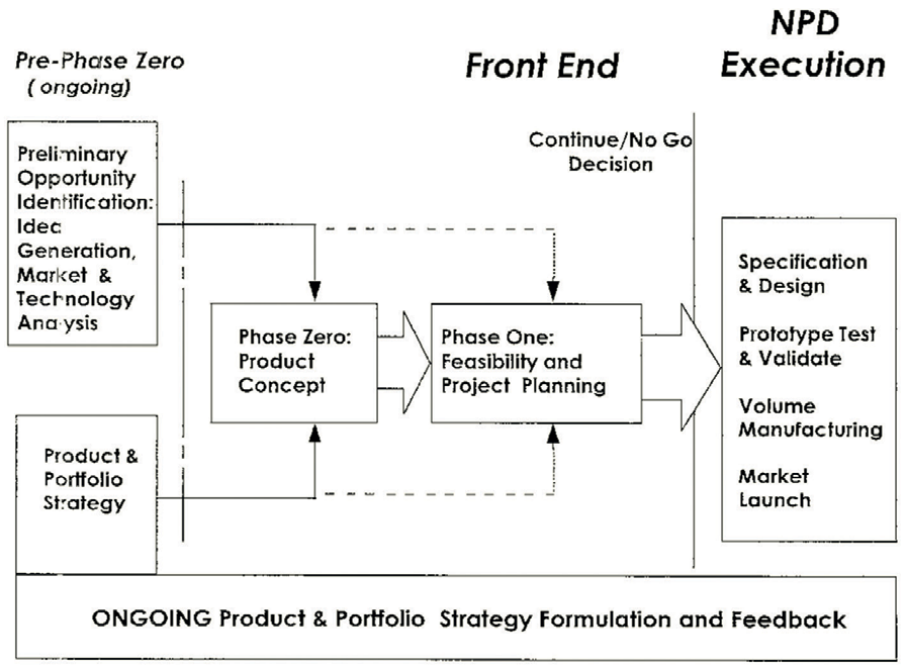

Figure 3.
Three Phase Front End model. Source: Khurana and Rosenthal [11].

- *Phase Zero*: This phase is initiated when Pre-Phase Zero identifies a promising opportunity. Its primary objective is to define the concept of a new product.

- *Phase One*: Following the conceptualization of the new product, Phase One focuses on analyzing feasibility and planning the project to initiate the NPD

process formally. It is crucial to maintain a constant interface with the organization's product and portfolio strategy throughout the entire process.

The New Concept Development (NCD) model, proposed by Koen et al. [14, 15], is a theoretical construction composed of the three fundamental concepts: controllable activities, "engine" and influencing factors. Controllable activities represent the elements that the organization can control. The "engine" encompasses the controllable aspects of the organization that are responsible for driving the activities of the FEI. Finally, the influencing factors are variables that have an impact on the FEI and are relatively outside of the organization's control [14, 15]. **Table 2** details the structure of the NCD model. In the structure of the NCD model, organizational capabilities are classified as an influencing factor because they usually change very slowly and are therefore uncontrollable. Alternatively, organizational capabilities can be incorporated into the "engine" to the extent that the organization can modify and control them [14].

The model proposed by Reid and De Brentani [19] provides a unique focus on disruptive innovations, highlighting their distinct entry into the organization compared to incremental innovations. According to this model, disruptive innovations typically originate from the external environment. **Figure 4** illustrates how the front end of the innovation process initiates its flow based on information from the external environment, involving the identification of unstructured problems and the recognition of opportunities. This model emphasizes that disruptive innovations follow a distinctive path, with the FEI process being strongly influenced by external inputs. The opportunities identified undergo thorough analyzes and decisions at various organizational levels before being formally integrated into an NPD project [19].

The seminal models presented – Cooper's Stage-Gate Model, Khurana, and Rosenthal's Three Phase Front End Model, Koen et al.'s New Concept Development (NCD) Model, and Reid and De Brentani's Model for Discontinuous Innovations – vary in focus, approach, depth, and structuring of activities. Despite these differences, a common thread emerges as they collectively address the FEI through key activities: identification and analysis of opportunities, generation, enrichment, and screening of ideas, product concept definition, and consideration of influencing factors

Concepts	Elements
Controllable activities	Opportunity identification Opportunity Analysis Idea generation Idea enrichment Idea selection Concept definition
"The engine"	Culture Leadership Business strategy
Influencing factors	Organizational capabilities The outside world Customer and competitor influences Enabling sciences and technology

Source: Koen et al. [14].

Table 2.
Structure of the NCD model.

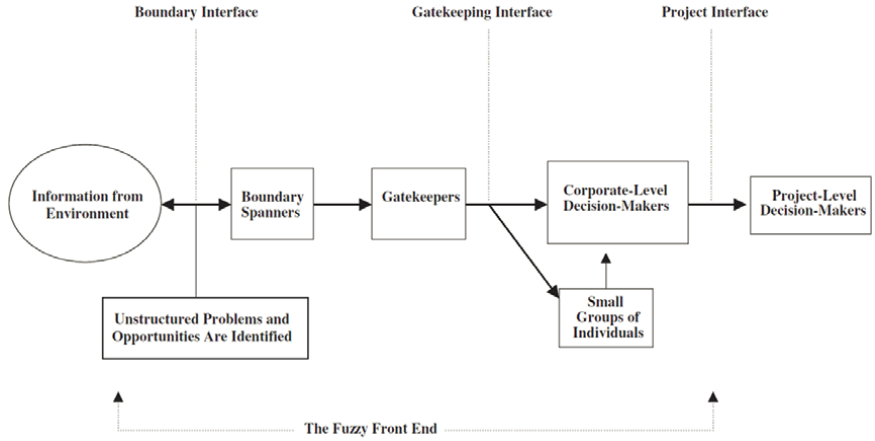

Figure 4.
The Fuzzy Front End of new product development for discontinuous innovations. Source: Reid and De Brentani [19].

(encompassing the outside world, market and technology information, scenario planning, competitive analysis, and organizational issues such as culture, leadership, strategy, portfolio, and capabilities).

The ultimate objective of these FEI activities is to formulate a well-defined product concept before entering the formal NPD stage. **Table 3** establishes the correspondence between FEI activities and the structures of the seminal models.

To mitigate potential ambiguities in the interpretation of certain terms related to the FEI, **Table 4** provides standardized reference definitions. This table serves as a reference guide, providing clear and standardized definitions for key terms associated with the FEI, enhancing clarity and consistency in their interpretation.

2.3 Defense sector

The defense sector holds strategic importance for nations, embodying a comprehensive "set of attitudes, measures, and actions undertaken by the State, with an emphasis on the military expression of the power, to safeguard national territory, sovereignty, and national interests against predominantly external threats, whether potential or manifest" ([24], p. 77). Characterized by complexity, the defense sector exhibits key features:

- *High technological level*: The defense industry requires substantial investments in research, development, and innovation to create sophisticated products such as aircraft, ships, weapons, and systems. These must operate safely and reliably under severe conditions [25], often characterized as Complex Products and Systems (CoPS). CoPS involve customization, production in small quantities by a few companies, integration of diverse knowledge areas, and a lifecycle spanning decades [26].

- *Technological duality*: Innovations developed for military purposes may have civilian applications (spin-off) and vice versa (spin-in) [27, 28]. Dual-use technologies, like GPS and the Internet, initially developed for defense, now find widespread civilian applications.

Activities	Structure of the seminal models
Identification and analysis of opportunities	• Discovery [17] • Pre-Phase Zero [11] • Identification and analysis of opportunities [14] • Boundary interface [19]
Generation, enrichment, and screening of ideas	• Discovery and idea screening [17] • Pre-Phase Zero [11] • Generation, enrichment, and selection of ideas [14] • Gatekeeping interface [19]
Product concept definition	• Scoping and build business case [17] • Phase Zero and Phase One [11] • Concept definition [14] • Project interface [19]
Consideration of influencing factors The outside world, market and technology information, scenario planning, competitive analysis, and organizational issues (culture, leadership, strategy, portfolio, and capabilities)	• Strategic, feasibility, market, technical, operational, and financial criteria [17] • Technological and market analysis, and product & portfolio strategy [11] • Organizational capabilities, the outside world, customer and competitor influences, enabling sciences and technology, and "the engine" – culture, leadership, and business strategy [14] • Environmental information, and scenario analysis at the corporate and project levels [19]

Table 3.
FEI activities and their relationship with the seminal models.

- *Governmental dependence*: The defense market is highly regulated and relies on government contracts, resulting in a strong dependence on public resources. From a demand perspective, the defense market operates as a monopsony, with the State being the primary purchaser of goods and services [29–31].

- *High market concentration*: Global defense market dominance by a few companies leads to limited competition and protectionist practices. Oligopolies in the defense market can collude, manipulate prices, limit competition, or engage in practices like dumping [32] to control strategic interests [31, 33].

- *Vulnerability to geopolitical issues*: The demand for defense equipment is influenced by geopolitical conflicts and international relations, resulting in a volatile market subject to sudden changes. Companies may exploit geopolitical issues for financial or strategic reasons, impacting commitments during times of national crisis [31, 34].

In summary, the defense sector is characterized by its strategic importance, technological advancement, dual-use nature, governmental dependence, market concentration, and vulnerability to geopolitical issues. This situation is a combination of a monopoly/oligopoly, where a few major global players dominate the supply, and a

Term	Definition
Opportunity	"A business or technology gap, that a company or individual realizes, that exists between the current situation and an envisioned future in order to capture competitive advantage, respond to a threat, solve a problem, or ameliorate a difficulty" ([14], p. 7).
Ideia	"The most embryonic form of a new product or service. It often consists of a high-level view of the solution envisioned for the problem identified by the opportunity" ([14], p. 7).
Product concept	"A well-defined form, including both a written and visual description, that includes its primary features and customer benefits combined with a broad understanding of the technology needed" ([14], p. 7).
The outside world	"Distribution channels, law, government policy, customers, competitors, and political and economic climate" ([14], p. 8).
Organizational culture	"A pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems" ([21], p. 17).
Organizational leadership	"It is originally the source of the beliefs and values that get a group moving in dealing with its internal and external problems" ([21], p. 36). "Leadership is needed to help the group identify the issues and deal with them" ([21], p. 407).
Organizational strategy	"A shared understanding of core mission, primary task, and manifest and latent functions" ([21], p. 88).
Organizational portfolio	"Collection of projects, programs, and other activities that are grouped together to meet strategic business objectives. The practice of portfolio management is integral to the implementation of an organization's overall strategic plan" [22].
Organizational capacity	In the context of dynamic capabilities theory, it is defined as "the firm's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments" ([23], p. 516).

Table 4.
Definitions for terms related to the FEI.

monopsony, where the State centralizes the demand. Recognizing these peculiarities highlights the need for a comprehensive exploration of FEI dynamics within the defense sector.

3. Methodology

In conducting this literature review, a comprehensive search strategy was employed, encompassing both academic and gray literature, as recommended by Thomé et al. [35]. The initial approach involved the following strategies for searching academic literature:

- *Databases*: Scopus and Web of Science (WoS), aligning with the methodology outlined by Ferreira et al. [36].

- *Search string*: The search string was crafted by combining key terms related to the FEI and the defense sector. The FEI-related terms were derived from a frequency analysis of authors' keywords, following the methodology of Ferreira et al. [36]. To capture the comprehensive scope of the defense sector, terms related to aerospace were also incorporated, acknowledging that certain countries treat both

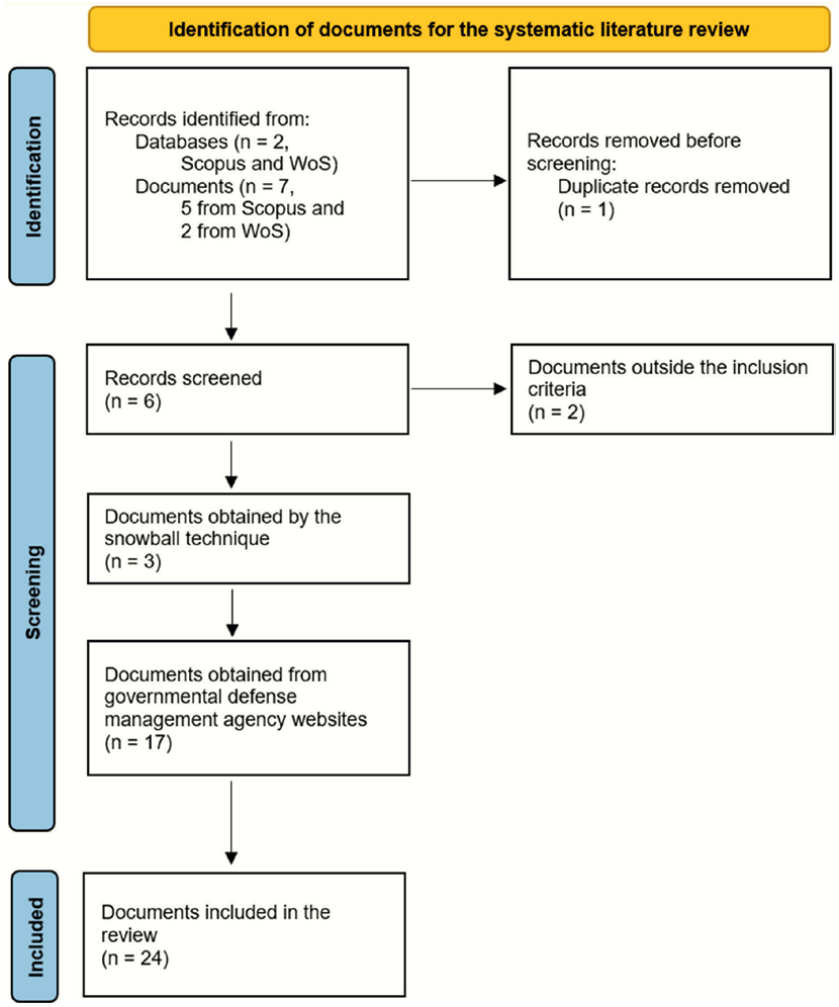

Figure 5.
Stages of the systematic literature review. Source: Adapted from Page et al. [38].

topics as a unified strategic theme. For instance, the United States has the U.S. Space Force under its Department of Defense [37]. The search was conducted on September 21, 2023, focusing on terms found in the title, abstract, and keywords:

- Scopus database: *TITLE-ABS-KEY((“front end of innovation” OR “front-end of innovation” OR “front end innovation” OR “front-end innovation” OR “fuzzy front end” OR “fuzzy front-end”) AND (“military” OR “defense” OR “defense” OR “navy” OR “army” OR “air force” OR “aerospace” OR “aeronautic*” OR “astronautic*” OR “avionics”)).*

- WoS database: *TS = ((“front end of innovation” OR “front-end of innovation” OR “front end innovation” OR “front-end innovation” OR “fuzzy front end” OR “fuzzy front-end”) AND (“military” OR “defense” OR “defense” OR “navy” OR “army” OR “air force” OR “aerospace” OR “aeronautic*” OR “astronautic*” OR “avionics”)).*

- *Inclusion criteria*: publications in English, Portuguese, or Spanish were considered, and the accessibility of the entire document was taken into account. Additionally, the publication had to address explicitly the FEI in the defense context.

The academic literature search yielded five documents from the Scopus database and two from WoS. Upon analysis, one redundancy was identified, resulting in six unique documents. Subsequently, it was observed that two articles did not meet the inclusion criteria, leaving four documents within the review scope. Following this initial search, the snowball technique was applied to identify relevant documents citing or cited by the selected publications. Additional efforts were made to explore works authored by the selected publications' authors, uncovering three more documents.

In parallel with the academic literature search, the exploration of government defense management agencies' websites led to the identification of 17 more documents. Therefore, while the academic literature contributed documents presenting general aspects of FEI in the defense sector, the gray literature addressed defense management in specific nations, ensuring representation across continents and encompassing both developed and developing countries. The nations (or alliances) covered included Australia, Brazil, China, India, NATO (North Atlantic Treaty Organization), the United Kingdom, the United States, and South Africa.

Thus, a total of 24 documents were selected for review. It is noteworthy that, during the research, no review works similar to this article were found. The steps of the review are represented in summary in **Figure 5**, using the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) diagram, a tool for presenting the flow of information through the different phases of a systematic literature review [38].

4. Front end of innovation in the defense sector

The investigation of FEI in the defense sector is structured based on content mapping of the selected review documents, focusing on key FEI activities outlined in Section 2.2. These activities include the identification and analysis of opportunities; generation, enrichment, and screening of ideas; product concept definition; and consideration of influencing factors.

4.1 Identification and analysis of opportunities

The identification and analysis of opportunities serve as the primary catalyst for the FEI process. It occurs when an organization recognizes a gap, whether related to business or technology issues. This gap represents the difference between the current state and a desired future state, presenting an opportunity that can be exploited to gain a competitive advantage, address a threat, solve a problem, or enhance a situation [14]. As stressed by Khurana and Rosenthal [11], the phase of identifying and analyzing opportunities should be an ongoing and continuous process within an organization.

In the defense sector, the identification and analysis of opportunities are intricately tied to Capability-Based Planning (CBP), a central process in strategic defense management [39, 40]. This strategic planning paradigm, initially utilized in the

United States Nuclear Program during the 1960s, saw broader adoption by the U.S. Department of Defense in 2001, becoming a reference for armed forces worldwide [41]. From this standpoint, **Table 5** provides a mapping of the phase of identification and analysis of opportunities within the documents reviewed.

Documents	Approaches	National context
United States [42]	CBP is implemented through the Joint Capabilities Integration and Development System (JCIDS). The strategic approach begins by identifying scenarios for the U.S. Armed Forces' operations. Then, the necessary capabilities for each scenario are determined. Finally, existing capabilities are evaluated, and gaps are identified (a process called Capabilities-Based Assessment – CBA). The assessment of capabilities follows the acronym DOTmLPF-P, which incorporates the following elements: Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy.	USA
NATO [43]	CBP is implemented following the acronym DOTMLPF-I, which incorporates the following elements: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability. Notably, the interoperability element is included in the approach, considering NATO comprises 32 member countries, listed alphabetically as follows: Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, the Netherlands, the United Kingdom, and the United States.	NATO
United Kingdom [44]	Implements CBP following the DLOD concept, referring to Defense Lines of Development. DLOD encompasses Training, Equipment, Personnel, Information, Doctrine & Concepts, Organization, Infrastructure, Logistics, and Interoperability. The latter is only sometimes listed as a separate line of development but is essential for combined operations with allies.	United Kingdom
Australia [45]	Implements CBP following the FIC concept, which stands for Fundamental Inputs to Capability. FICs include Organization, Command and management, Personnel, Collective training, Major systems, Facilities and training areas, Supplies, Support, and Industry.	Australia
Barton [46]	Implements CBP similarly to the U.S. DOTmLPF-P approach.	China
India [47] and South Africa [48]	They highlight the capability-based approach without defining specific analysis elements.	India and South Africa
Brasil [49, 50]	CBP is implemented following the acronym DOAMEPI, which includes the following elements: Doctrine, Organization (and/or processes), Training, Materiel, Education, Personnel, and Facilities. It is worth noting that Brazil maintains a capabilities catalog to support its CBP.	Brazil
Helfat and Peteraf [51], Salvato and Rerup [52], and Wallin et al. [53]	They emphasize the importance of the capability-based approach in supporting planning for the development of new technological products.	Generic (academic literature)

Table 5.
Approaches to identification and analysis of opportunities within the review documents.

4.2 Generation, enrichment, and screening of ideas

According to Koen et al. [14], the generation and enrichment of ideas follow the identification and analysis of opportunities. An idea, as conceptualized by the authors, represents the most preliminary form of a new product or service, typically outlining a high-level vision for the planned solution related to the identified opportunity [14]. Cooper [17], in the stage-gate model, underscores that ideas for new products must undergo initial screening, known as gate 1, before being integrated into an organization's project [17]. Reid and De Brentani [19] also stress the importance of a formal analysis of opportunities/ideas at the corporate level before progressing to the project level [19].

In the defense sector, as outlined in **Table 6**, the identification of the need for a new product occurs when a capability gap analysis indicates the necessity for a new materiel solution. This triggers the formal process of acquiring a defense product. **Table 6** provides a mapping of the phase of generation, enrichment, and screening of ideas within the reviewed documents.

4.3 Product concept definition

According to Koen et al. [14], a well-defined product concept should entail a comprehensive configuration, offering both written and visual descriptions that encapsulate the primary features, customer benefits, and a broad understanding of the required technologies. This stage in product development represents the final step preceding the formal NPD process [14]. The models proposed by Khurana and Rosenthal [11], Reid and De Brentani [19], and Cooper [17] also emphasize the

Documents	Approaches	National context
United States [42, 54]	The American approach prioritizes non-materiel solutions when addressing capability gaps, incorporating adjustments in Doctrine, Organization, Training, Leadership and education, Personnel, Facilities, and/or Policy (DOTmLPF-P). The lowercase "m" in the acronym signifies this approach. If a materiel solution is deemed necessary, an Initial Capabilities Document (ICD) is drafted, justifying the need for a new acquisition process. The ICD outlines the identified capability gap, the concept of operations (CONOPS) detailing the expected operational context of the materiel solution, and associated risks. A validated ICD is mandatory for a Materiel Development Decision (MDD), initiating the life cycle of the new product.	USA
United Kingdom [44]	Following a model similar to that of the USA, the identification of the need for a materiel solution and the elaboration/approval of the concept of operations initiate the life cycle of a new product.	United Kingdom
Australia [45]		Australia
India [47]		India
South Africa [48]		South Africa
Brasil [55]		Brazil

Table 6.
Approaches to idea generation, enrichment, and screening within the review documents.

Documents	Approaches	National context
United States [42, 54]	The US approach divides the life cycle of a defense product into six phases: Materiel Solution Analysis (MSA), Technology Maturation & Risk Reduction (TMRR), Engineering & Manufacturing Development (EMD), Production & Deployment (PD), Operations & Support (OS), and Disposal. The FEI phases (before NPD), MSA and TMRR, involve significant requirements engineering effort. MSA uses the CONOPS to define operational requirements, establishing operational performance parameters and attributes – Key Performance Parameters (KPPs) and Key System Attributes (KSAs). The physical description is preliminary, analyzing technical alternatives for product acquisition. MSA concludes with the approval of the Capability Development Document (CDD) Draft. The CDD Draft evolves during the TMRR phase, refining technical product requirements into the Request For Proposals (RFP), inviting companies to submit development proposals. TMRR concludes with the approval of the Preliminary Design Review (PDR), ensuring technological risks are mitigated and the product concept is ready to advance to the formal NPD stage.	USA
Innovations [60] and United Kingdom [44]	Divide the product life cycle into six phases: concept, assessment, demonstration, manufacture, in-service, and disposal. The FEI phases are concept and assessment. The concept phase develops the logical and physical descriptions of the product. The subsequent phase refines these descriptions through evaluations for risk reduction before entering NPD. Risk reduction is exemplified by technology competitions promoted by the UK Ministry of Defense to mature/identify alternatives for technological components of the product before its development/integration.	United Kingdom
Australia [45]	Divides the product life cycle into five phases: Strategy and Concepts, Risk Mitigation and Requirement Setting, Acquisition, In-Service, and Disposal. The FEI phases are Strategy & Concepts and Risk Mitigation & Requirement Setting. These phases define the logical and physical descriptions of the product and conduct risk reduction activities before entering NPD.	Australia
India [47]	Adopts distinct workflows depending on the acquisition modality: Buy, Buy and Make, Leasing, Make, Design and Development, and Strategic Partnership Model. In all cases, logical and physical descriptions are developed, in greater or lesser detail, to support the acquisition of a defense product.	India
South Africa [48]	Divides the life cycle of a defense product into four phases: Design, Development, Operation & Maintenance, and Disposal. The phase belonging to the FEI is the Design phase, where the product concept is developed before entering NPD.	South Africa
Brasil [55]	Divides the life cycle of a defense product into five phases: conception, acquisition, production, operation and support, and disposal. The phase belonging to the FEI is conception. The most important step of the conception phase is integrated design, which establishes the logical description (doctrinal/operational constraints and operational requirements) and the physical definition (technical requirements, conceptual design, technology map, integrated logistics support plan, and test and evaluation plan) of the product before entering NPD.	Brazil
Clegg et al. [61], Larsson et al. [62] and Johansson et al. [63]	In the aerospace and defense context, they present simulators or methodologies to support collaborative product concept development before entering NPD.	Generic (academic literature)

Table 7.
Approaches to product concept definition within the review documents.

significance of product concept development, feasibility analysis, project planning, and decision-making as crucial prerequisites before formally entering the NPD phase.

In the defense sector, the Armed Forces commonly adopt the systems engineering lifecycle concept to structure their acquisition processes [56]. Within this framework, the product concept undergoes development through a top-down approach, comprising two distinct phases: logical description (problem domain) and physical description (solution domain). The logical or functional description essentially outlines the intended functionalities of the new product from the user's perspective, providing an operational view. Building upon the logical description, the physical description then defines the high-level architecture of the product elements, encompassing systems, subsystems, assemblies, and/or components, from a technical perspective [57–59]. **Table 7** provides a mapping of the product concept definition phase within the reviewed documents.

4.4 Consideration of influencing factors

According to Koen et al. [14], influencing factors are variables that impact FEI and are relatively outside the organization's control. **Table 8** maps the influencing factors considered in the review documents.

5. Discussion

After presenting the review results, it is essential to delve deeper into key findings and considerations identified throughout the study.

5.1 Synthetic diagnosis of the results

Table 9 provides a condensed overview, offering a synthetic diagnosis of the results derived from the review. It succinctly outlines FEI activities in the defense sector and establishes connections with the influencing factors under consideration.

5.2 Peculiarities of FEI in the defense sector

After systematically mapping the FEI in defense sector against established FEI models, several distinct aspects specific to the military context have emerged, as shown in **Table 10**.

5.3 Contributions to the FEI literature

The exploration of Scopus and WoS databases revealed a noteworthy observation: the existing academic literature has not systematically delved into the realm of Front End of Innovation (FEI) within the defense sector. In dissecting the distinct aspects of the initial phase of the military innovation process, several novel points of analysis emerged, each offering unique insights not extensively addressed in seminal FEI models. These include:

- *Use of systems engineering approach*: The defense sector prominently employs systems engineering activities during the early phase of military innovation. This

Documents	Influencing factors	National context
United States [42, 54, 64, 65]	National guidelines (notably the National Security Strategy – NSS), budget management (PPBE process – Planning, Programming, Budgeting, and Execution), scenario planning, and the strategic portfolio of programs/projects/capabilities. Emphasis on analyzes of alternatives, feasibility, technological criticality (list of critical and emerging technologies), and technological maturity (TRL - Technology Readiness Levels of 6 or higher as reference value before entering NPD). Selection and continuity of leadership (military and/or civilian) in NPD project planning.	USA
NATO [43]	Emphasizes interoperability as a relevant factor, considering it integrates 32 member countries.	NATO
United Kingdom [44, 66]	Technological criticality (critical technological areas guided by the "Integrated Force Plan 2030") and technological maturity (TRL 7 and SRL – System Readiness Level – 4 as reference values before entering NPD). Continuity management in NPD project planning.	United Kingdom
Australia [67, 68]	Government Office for Critical Technologies Policy Coordination periodically publishes a list of technologies to be prioritized in national technological projects, especially in the defense area. Action plan for the development of technological products to ensure mastery of critical technological areas.	Australia
IEDI [69]	Defines "frontier" technologies to reduce dependence on foreign components and supply chains in these areas. Emphasis on dual-use technologies, especially in basic research phases, where it is possible to circumvent international embargoes and undertake research in critical areas with developed countries.	China
India [47]	Emphasizes critical technological areas following "Make" or "Buy and Make" strategies. The Indigenous Content (IC) factor specifies the percentage that defense technological capability acquisition contracts should allocate to national investments.	India
South Africa [48]	Defines key areas to be prioritized in the development of the defense industrial base to reduce technological dependency.	South Africa
Brasil [55, 70]	Technological criticality (priority areas defined in the strategic plan) and technological maturity (product development must have critical component technologies with a TRL of 6 or higher). The concept of technological duality gains importance for extra-budgetary resources and the integration of military and civilian sectors.	Brazil

Table 8.
Influencing factors within the review documents.

approach encompasses requirements engineering and systems lifecycle management, aspects not explicitly emphasized in traditional FEI models.

- *Relevance of technological duality, criticality, and maturity*: Concepts such as technological duality, criticality, and maturity play a crucial role in military FEI. These factors, while not extensively covered in established FEI models, are instrumental in decision-making processes, risk mitigation, and the strategic development of defense capabilities.

- *Organizational capabilities as the "engine" of FEI*: In contrast to seminal NPD models that classify organizational capabilities as influencing factors, the defense

Activity	Description	Influencing factors
Identification and analysis of opportunities	• Identification of capability gap within CBP. • The analysis considers the following elements: doctrine, organization, training, materiel, leadership and education, personnel, facilities, logistics, interoperability, and policy.	National guidelines, public budget, scenario planning, geopolitical issues, and strategic portfolio.
Generation, enrichment, and screening of ideas	• When analyzing a capability gap, if a materiel solution is the only way to fill it, it is necessary to justify and develop the concept of operations for that solution (what is expected from the materiel solution in the operational context). • The approval of the concept of operations initiates the life cycle of the new product.	
Product concept definition	• The product concept is developed in a top-down approach divided into two stages: logical description (problem domain) and physical description (solution domain). • The logical or functional description essentially defines what the new product should be able to do from the user's perspective. It usually relies on the concept of operations to elicit the product's operational requirements, establishing parameters and attributes of operational performance. • Based on the logical description, the physical description defines the high-level architecture of the product elements (systems, subsystems, assemblies, and/or components) from a technical perspective. The physical description is generally represented by the product's technical requirements. • The physical description underpins the mapping of component technologies; the decision on the acquisition model (purchase and/or research and development); the signing of supply, development, and/or integration contracts; and the planning of the acquisition project. • The approval of the product concept initiates the formal NPD stage.	• Analyzes of alternatives, feasibility, technological criticality, technological maturity, and possible use of the concept of technological duality for capturing extra-budgetary resources and integrating military and civilian sectors. • Planning of the NPD project (scope, cost, time, life cycle, and leadership continuity).

Table 9.
FEI activities in the defense sector.

sector integrates organizational capabilities as a fundamental component of the FEI "engine." Capability-based planning is a central element in identifying and analyzing opportunities, as well as in generating, enriching, and screening ideas.

Aspect	Military FEI	Seminal FEI models
Systems engineering approach	Government documents highlight the prevalent use of systems engineering activities, particularly in requirements engineering and systems lifecycle management, during the early phases of military innovation.	Often, they overlook the systems engineering approach, emphasizing the need for innovation models tailored to the defense sector.
National strategic focus	The optimization of FEI primarily serves the common good, development, and survival of the State, differing from the profit-driven motives of commercial entities. Consideration of geopolitical aspects and alignment with high-level national guidelines becomes crucial in this context.	Generally designed for technology product manufacturing companies, lacking emphasis on the broader national scope inherent in defense innovation.
Technological duality	The defense sector incorporates the concept of technological duality, where innovations or technologies intended for military use may find civilian applications (spin-off), and vice versa (spin-in). This dual-use perspective is essential in the defense sector, influencing decisions on resource allocation and fostering collaboration between military and civilian technological advancements.	The emphasis is typically on generating ideas and concepts within a specific industry or market to meet customer needs or address market gaps. The models may not explicitly consider the dual-use potential or the transferability of technologies between military and civilian domains.
Technological criticality	FEI in the military context is closely tied to the concept of technological criticality. Investments in defense prioritize mapping critical technological areas to promote strategic sectors in the national industrial base.	The strategic mapping of critical technologies for national development, as seen in the defense sector, is a specific consideration that goes beyond the scope of traditional FEI models.
Technological maturity	Defense innovation involves assessing the maturity of critical technologies to mitigate risks before entering the formal NPD stage. The TRL scale is commonly used for this assessment. The TRL scale, and in some cases, the SRL, plays a crucial role in gauging the readiness of critical technologies, ensuring they meet the required standards before advancing to NPD.	While traditional FEI models may indirectly touch upon aspects of technology readiness, they typically do not incorporate a formalized assessment process like the TRL scale. The emphasis in traditional FEI models is often on customer-centric aspects, market dynamics, and the development of innovative solutions.
Organizational capabilities as the "engine"	FEI, in defense, places organizational capabilities at the core, considering capability-based planning as a central element in identifying and analyzing opportunities, as well as in generating, enriching, and screening ideas. Organizational capabilities are integral to the military FEI "engine," contradicting the notion that they change slowly and are uncontrollable.	Organizational capabilities are classified as an influencing factor and not as part of the FEI's "engine", considering that they usually change very slowly and are therefore uncontrollable.

Aspect	Military FEI	Seminal FEI models
"Implementation" of innovation	In defense, the concept of "implementation" extends beyond market introduction. It is realized when a new product is effectively incorporated into the capability's portfolio of an Armed Force, necessitating adjustments in various non-technological aspects. The symbiosis between technological and doctrinal advancements defines military innovation, emphasizing the harmonization of both aspects for successful implementation.	It aligns with the definition from the Oslo Manual [71] which asserts that the "implementation" of a product innovation is realized when a new or significantly improved product is introduced to the market, i.e., is commercialized.
Continuity in project leadership	Project leadership continuity is a crucial influencing factor, given the extended duration of defense product development and high turnover among military leaders. Mitigating leadership turnover is addressed through strategies like the continuity of civilian leadership, ensuring stability throughout the NPD phase.	They emphasize the significance of organizational leadership in the context of the FEI, but do not explicitly address managing leadership continuity in NPD project planning.

Table 10.
Peculiarities of FEI in the defense sector.

- *"Implementation" of military innovation*: The implementation of military innovation necessitates a broader interpretation compared to traditional FEI models. In defense, implementation occurs when a new or improved product is seamlessly integrated into the capability's portfolio of an Armed Force. This integration involves adjustments in various non-technological aspects, emphasizing the symbiosis between technological and doctrinal advancement.

- *Continuity in project leadership*: Recognizing the high turnover of military leaders and the extended durations of defense projects, the continuity of leadership emerges as a critical consideration. Seminal FEI models do not explicitly address managing leadership continuity in NPD project planning.

Moreover, it is noteworthy that recent contributions in the FEI literature have started to delve deeper into the alignment between organizational strategy and FEI activities. Unlike seminal models that treat this issue generically, recent works, such as the integrative ontologies developed by Pereira et al. [20] and Castro and Ferreira [72, 73], provide management artifacts designed to align organizational strategic vision with FEI activities. Employing the design science paradigm, these artifacts integrate constructs, models, methods, and instantiations, thereby enriching the strategic dimension of FEI literature.

5.4 Contributions to the defense literature

The defense sector, encompassing products ranging from CoPS to mass-produced items, presents a unique challenge due to its diverse complexity and production

volume [74]. While the CoPS research area has an established connection with systems engineering literature, the realm of mass-produced products aligns more closely with the theoretical foundations of the FEI literature. Notably, defense documents predominantly draw from the CoPS approach, sparingly incorporating principles from mass production. However, recognizing that the military context spans both worlds, the integration of these approaches becomes crucial, and mapping established FEI models within the dynamics of the initial phase of the military innovation process serves as a valuable step in achieving this harmonization.

Moreover, the FEI literature, characterized by well-defined seminal models and recent integrative ontologies (as discussed in the previous section), contrasts with the more heterogeneous nature of the systems engineering literature. The latter encompasses diverse authors, countries, organizations, and standardization bodies, each adhering to distinct management models with unique nomenclatures and structures [43–45, 47, 48, 54, 55, 57–59]. In this context, the FEI literature emerges as a unifying force, facilitating the creation of a common representation of knowledge related to the early stage of the military innovation process. This not only streamlines communication among specialists, decision-makers, managers, researchers, entrepreneurs, and other stakeholders in the defense field but also promotes greater efficiency in navigating the diverse landscape of defense innovation.

5.5 Limitations

Several limitations were identified during this research:

- *Selection of seminal FEI models*: The identification of seminal FEI models relied on findings from Pereira et al. [12, 20] and co-citation analysis of FEI-related works available in the Scopus and WoS databases. Alternative criteria for model selection might yield a different set of seminal documents, potentially influencing the analysis.

- *Data collection in gray literature*: The exploration of gray literature related to FEI in the military sector was constrained by the availability of documents on government websites of defense management agencies. This limitation could result in an incomplete representation of the landscape.

- *Scope of mapping*: The review presented an initial mapping of FEI in the defense sector within seminal models. A more comprehensive and structured mapping could be achieved through the adoption of more robust methodological approaches, such as the design science paradigm [75, 76]. This suggests that there is potential for a more in-depth and detailed examination of FEI activities in the defense sector.

Acknowledging these limitations is essential for a nuanced understanding of the scope and implications of the study, guiding future research endeavors in this domain.

6. Conclusion

This study aimed to comprehensively explore the dynamics of FEI in the defense sector through a systematic review encompassing 24 documents from both academic

and gray literature. By analyzing seminal FEI models, the research mapped key activities within the defense context, including the identification and analysis of opportunities, generation, enrichment, and screening of ideas, product concept definition, and consideration of influencing factors.

The study's contributions extend to both FEI and defense literature, introducing original perspectives. Notably, it emphasized the systems engineering approach, national strategic focus, technological duality, technological criticality, technological maturity, organizational capabilities as the "engine", the unique concept of "implementation" in military innovation, and the importance of continuity in project leadership.

Acknowledging limitations, such as the criteria for selecting seminal FEI models, constraints in accessing gray literature, and the preliminary nature of the mapping, the study calls for future research to employ more robust methodologies, like the design science paradigm [75, 76], for an in-depth understanding of the initial phase of the military innovation process.

In conclusion, this research lays a foundation for further exploration and synthesis of knowledge, contributing to the advancement of both FEI theory and its application in the defense sector.

Acknowledgements

This work was supported by the Brazilian Army (Atv PCENA V23-011).

We thank Dr. João José Pinto Ferreira (INESC TEC and Faculty of Engineering, University of Porto) for his expertise and help in writing the manuscript.

Author details

Romullo Girardi[1,2*], Juraci Ferreira Galdino[1] and Paulo César Pellanda[1]

1 Military Institute of Engineering, Rio de Janeiro, Brazil

2 INESC TEC and Faculty of Engineering, University of Porto, Porto, Portugal

*Address all correspondence to: romullogirardi@ime.eb.br

References

[1] Tidd J, Bessant J. Managing Innovation: Integrating Technological, Market and Organizational Change. 7th ed. Hoboken, USA: Wiley; 2020

[2] Keeley L, Walters H, Pikkel R, et al. Ten Types of Innovation: The Discipline of Building Breakthroughs. 1st ed. Hoboken, USA: Wiley; 2013

[3] Boeddrich H-J. Ideas in the workplace: A new approach towards organizing the fuzzy front end of the innovation process. Creativity and Innovation Management. 2004;**13**:274-285

[4] Koen P, Bertels H, Kleinschmidt E. Managing the front end of innovation - Part I: Results from a three-year study. Research-Technology Management. 2014;**57**:34-43

[5] Koen P, Bertels H, Kleinschmidt E. Managing the front end of innovation - Part II: Results from a three-year study. Research-Technology Management. 2014;**57**:25-35

[6] Markham SK. The impact of front-end innovation activities on product performance. Journal of Product Innovation Management. 2013;**30**:77-92

[7] Stevens GA, Burley J. Piloting the rocket of radical innovation. IEEE Engineering Management Review. 2004;**32**:16-25. DOI: 10.1109/EMR.2004.25114 [Epub ahead of print]

[8] Verworn B, Herstatt C, Nagahira A. The fuzzy front end of Japanese new product development projects: Impact on success and differences between incremental and radical projects. R&D Management. 2008;**38**:1-19

[9] Williams MA, Kochhar AK, Tennant C. An object-oriented reference model of the fuzzy front end of the new product introduction process. International Journal of Advanced Manufacturing Technology. 2007;**34**:826-841

[10] Khurana A, Rosenthal SR. Integrating the Fuzzy Front End of New Product Development. Cambridge, USA: MIT Sloan Management Review; 1997

[11] Khurana A, Rosenthal SR. Towards holistic 'front ends' in new product development. Journal of Product Innovation Management. 1998;**15**:57-74

[12] Pereira AR, Ferreira JJP, Lopes A. Front end of innovation: An integrative literature review. Journal of Innovation Management. 2017;**5**:22-39

[13] Smith PG, Reinertsen DG. Developing Products in Half The Time. New York: Van Nostrand Reinhold; 1991

[14] Koen P, Ajamian G, Boyce S, et al. Fuzzy front end: Effective methods, tools, and techniques. Industrial Research. 2002. pp. 5-35

[15] Koen P, Ajamian G, Burkart R, et al. Providing clarity and a common language to the 'fuzzy front end'. Research Management. 2001;**44**:46-55

[16] Kock A, Heising W, Gemünden HG. How ideation portfolio management influences front-end success. Journal of Product Innovation Management. 2015;**32**:539-555

[17] Cooper RG. Perspective: The stage-gates idea-to-launch process-update, what's new, and NexGen systems. Journal of Product Innovation Management. 2008;**25**:213-232

[18] Cooper RG. Stage-gate systems: A new tool for managing new products. Business Horizons. 1990;**33**:44-54

[19] Reid SE, De Brentani U. The fuzzy front end of new product development for discontinuous innovations: A theoretical model. Journal of Product Innovation Management. 2004;**21**:170-184

[20] Pereira AR, Ferreira JJP, Lopes A. A knowledge representation of the beginning of the innovation process: The front end of innovation integrative ontology (FEI2O). Data & Knowledge Engineering. 2020;**125**:1-20

[21] Schein EH. Organizational Culture and Leadership. 3rd ed. San Francisco, CA: Jossey-Bass; 2004

[22] PMI. The Standard for Portfolio Management. 2017. Available from: https://www.pmi.org/pmbok-guide-standards/foundational/standard-for-portfolio-management [Accessed: March 5, 2024]

[23] Teece DJ, Pisano G, Shuen A. Dynamic capabilities and strategic management. Strategic Management Journal. 1997;**18**:509-533. DOI: 10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z [Epub ahead of print]

[24] Brasil. Política Nacional de Defesa e Estratégia Nacional de Defesa. 2016

[25] Bitzinger RA. The Modern Defense Industry: Political, Economic, and Technological Issues. Westport, USA: Praeger Publishers; 2009

[26] Hobday M. Product complexity, innovation and industrial organisation. Research Policy. 1998;**26**:689-710

[27] Amarante JCA d. Processos de obtenção de tecnologia militar. In: Texto para discussão. Rio de Janeiro, Brasil: Instituto de Pesquisa Econômica Aplicada (Ipea); 2013. p. 1877

[28] Brustolin VM. Inovação e Desenvolvimento via Defesa Nacional nos EUA e no Brasil. Rio de Janeiro, Brasil: Universidade Federal do Rio de Janeiro e Universidade de Harvard; 2014

[29] Urbano EP. A contribuição dos offsets em defesa para a inovação e transferência de tecnologia para a base industrial de defesa. Brasília, Brasil: Universidade de Brasília; 2019

[30] Araujo BC, De Negri F, De Negri JA, et al. Base industrial de defesa. In: de Negri JA, Lemos MB, editors. O Núcleo Tecnológico da Indústria Brasileira. Brasília, DF: Ipea, FINEP e ABDI; 2011. pp. 595-653.

[31] Galdino JF, Schons DL. Maquiavel e a importância do poder militar nacional. Coleção Meira Mattos: revista das ciências militares. 2022;**16**:369-384

[32] Ethier WJ. Dumping. Journal of Political Economy. 1982;**90**:487-506

[33] Anderton CH. Economics of arms trade. In: Handbook of Defense Economics. Amsterdam, Netherlands: Elsevier; 1995. pp. 523-561

[34] da Silva CD. Planejamento Baseado em Capacidades e suas perspectivas para o Exército Brasileiro. Centro de Estudos Estratégicos do Exército - Artigos Estratégicos. 2019;**7**:21-29

[35] Thomé AMT, Scavarda LF, Scavarda AJ. Conducting systematic literature review in operations management. Production Planning and Control. 2016;**27**:408-420

[36] Ferreira JJP, Mention AL, Torkkeli M. Phrasing the giant: On the importance of rigour in literature search process. Journal of Innovation Management. 2020;**8**:1-10. DOI: 10.24840/2183-0606_008.002_0001 [Epub ahead of print]

[37] United States. Defense Space Strategy Summary. 2020.

[38] Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ. 2021;**372**:1-9. DOI: 10.1136/bmj.n71 [Epub ahead of print]

[39] Najgebauer A, Antkiewicz R, Chmielewski M, et al. The qualitative and quantitative support method for capability based planning. In: Intelligent Information and Database Systems. Bali, Indonesia: Springer; 2015. pp. 212-223

[40] Tagarev T. Capabilities-based planning for security sector transformation. Information & Security An International Journal. 2009;**24**:27-35

[41] United States. Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation. 2002

[42] United States. 5123.01H-Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS). 2018

[43] NATO. Joint Analysis Handbook. Lisbon, Portugal: NATO; 2016

[44] United Kingdom. Knowledge in Defence (KiD). 2019

[45] Australia. Defence Capability Manual. 2022

[46] Barton J. China's PLA Modernization through the DOTMLPF-P Lens. TRADOC Mad Scientist Laboratory; 2021. Available from: https://madsciblog.tradoc.army.mil/330-chinas-pla-modernization-through-the-dotmlpf-p-lens/

[47] India. Defence Acquisition Procedure 2020. 2020

[48] South Africa. South African Defence Review. 2015

[49] Brasil. EB20-MF-10.102 - Manual de Fundamentos da Doutrina Militar Terrestre. 2019

[50] Brasil. EB20-C-07.001 - Catálogo de Capacidades do Exército. 2014

[51] Helfat CE, Peteraf MA. The dynamic resource-based view: Capability lifecycles. Strategic Management Journal. 2003;**24**:997-1010

[52] Salvato C, Rerup C. Beyond collective entities: Multilevel research on organizational routines and capabilities. Journal of Management. 2010;**37**:468-490

[53] Wallin J, Parida V, Isaksson O. Understanding product-service system innovation capabilities development for manufacturing companies. Journal of Manufacturing Technology Management. 2015;**26**:763-787. DOI: 10.1108/JMTM-05-2013-0055 [Epub ahead of print]

[54] United States. 5000.85 - Major Capability Acquisition. 2020

[55] Brasil. EB10-IG-01.018 - Instruções Gerais para a Gestão do Ciclo de Vida dos Sistemas e Materiais de Emprego Militar. 2022

[56] Faulconbridge R, Ryan M. Introduction to Systems Engineering. Canberra: Argos Press; 2015

[57] Blanchard B, Fabrycky W. Systems Engineering and Analysis. 5th ed. Upper Saddle River, NJ: Prentice Hall; 2011

[58] International Council on Systems Engineering (INCOSE). INCOSE Systems Engineering Handbook. San Diego, USA: INCOSE; 2023

[59] International Organization for Standardization (ISO). ISO/IEC/

IEEE 15288 - Systems and Software Engineering - System Life Cycle Processes. Geneva, Switzerland: ISO; 2023

[60] Innovations. Competing for defence ideas: Looking wider for innovation. Strategic Direction. 2008;**24**:35-37. DOI: 10.1108/02580540810839359 [Epub ahead of print]

[61] Clegg B, Alexander I, Wingrove S, et al. Tool support for integrating extended enterprises. IEE Proceedings - Software. 2000;**147**:101-108. DOI: 10.1049/ip-sen:20000907 [Epub ahead of print]

[62] Larsson A, Larsson T, Bylund N, et al. Rethinking virtual teams for streamlined development. In: Torres-Coronas T, Macgregor SP, editors. Higher Creativity for Virtual Teams - Developing Platforms for Co-Creation. Hershey, USA: Information Science Reference; 2007. DOI: 10.4018/978-1-59904-129-2.ch007 [Epub ahead of print]

[63] Johansson C, Hicks B, Larsson AC, et al. Knowledge maturity as a means to support decision making during product-service systems development projects in the aerospace sector. Project Management Journal. 2011;**42**:32-50

[64] United States. Critical and Emerging Technologies List Update. 2022

[65] United States. Technology Readiness Assessment (TRA) Deskbook. 2009

[66] United Kingdom. The Defence Capability Framework. 2022

[67] Australia. Blueprint for Critical Technologies. 2021

[68] Australia. The Action Plan for Critical Technologies. 2021

[69] IEDI. O 14º Plano Quinquenal Chinês: Transformando a China em potência industrial e tecnológica. Carta do Instituto de Estudos para o Desenvolvimento Industrial-Edição 1094; 2021. Available from: https://iedi.org.br/cartas/carta_iedi_n_1094.html [Accessed: July 2, 2023]

[70] Brasil. Plano Estratégico do Exército 2020-2023. 2020

[71] Organização para a Cooperação e o Desenvolvimento Econômico (OCDE). Manual de Oslo: Diretrizes para a Coleta e Interpretação de dados sobre Inovação Tecnológica. Paris: OCDE; 2005

[72] Castro RN, Ferreira JJP. Project portfolio management in the front-end of innovation of research centers: A literature review. Technology Innovation Management Review. 2020;**10**:46-59

[73] Castro RN, Ferreira JJP. The front-end of R&D at non-profit research centers: How does research produce impact? International Journal of Innovation and Technology Management. 2023;**20**:1-22

[74] Girardi R, França Junior JA, Galdino JF. A customização de processos de avaliação de prontidão tecnológica baseados na escala TRL: Desenvolvimento de uma metodologia para o Exército Brasileiro. Coleção Meira Mattos: Revista das ciências militares. 2022;**16**:491-527. DOI: 10.52781/cmm.a084

[75] Hevner AR, March ST, Park J, et al. Design science in information systems research. MIS Quarterly: Management Information Systems. 2004;**28**:75-105

[76] Vaishnavi V, Kuechler B, Stacey P. Design Science Research in Information Systems. desrist.org - Design science research in information systems and technology; 2021. Available from: http://www.desrist.org/design-research-in-information-systems [Accessed: September 28, 2023]

Section 2

Case Studies: Countries' National Security in the Digital and Information Age

Chapter 4

The Israeli Media during the Gaza War: Insights from the First Weeks after the Disaster

Yuval Karniel and Amit Lavie-Dinur

Abstract

Since the tragic launch of the Israel—Hamas war (Gaza war) on October 7th, 2023, the role of Israeli media in shaping public discourse and national sentiment has been a subject of intense scrutiny. This article delves into the intricate relationship between media coverage and societal perceptions during the initial weeks following the terrorists' invasion. It explores how Israeli media navigated the complex terrain of war reporting, balancing the duty of factual reporting with national security concerns and the psychological impact on the civilian population. The study highlights the media's efforts to construct a narrative that not only informed the public but also fostered a sense of national unity and resilience. Through a comprehensive analysis of various media outlets, the article sheds light on the dynamics of media coverage in times of crisis, examining the interplay between journalistic practices, government policies, and public sentiment. This inquiry into the Israeli media's coverage of the Gaza war provides valuable insights into the power of the press in shaping public opinion during periods of national upheaval and the ethical challenges inherent in reporting on conflict and terrorism.

Keywords: Israeli media, Gaza war, war reporting, national sentiment, media and society, journalism ethics, conflict coverage, public opinion shaping, government-media relations, psychological impact of war news, trust in the media

1. Introduction

Media coverage plays a pivotal role in shaping public opinion about terrorist events. Some scholars emphasise the significant influence of media in forming societal perceptions and setting the public agenda. They argue that the media is a major force in moulding public opinion [1–3]. Likewise, Bruhn states that since major terrorist attacks such as those on September 11, as well as those in London, Madrid, and Oklahoma, the media, has significantly influenced the public's perception of terrorism [4]. Numerous academic studies have demonstrated that television coverage, particularly following the September 11 and Oklahoma attacks, leads to post-traumatic stress disorder and depression among civilians. Wilkinson views the media-terrorism relationship as symbiotic [5]. In alignment with Wilkinson, Burke

also acknowledges the evident connection between the media and terrorism, noting that terrorist groups often gain popularity through mass media exposure [6]. Michael Jetter's research indicates that suicide missions garner substantial media coverage, which may account for their growing appeal among terrorist organisations. Jetter advocates for the media to refrain from offering a platform for terrorists' propaganda [7]. Similarly, Yonah Alexander believes that the media serves as an effective tool for the propaganda and psychological warfare of terrorist groups [8].

This exploratory study embarks on a critical examination of the Israeli media's role during the Gaza war that launched on October 7, 2023. Despite extensive scholarship on the media's influence on public perceptions of terrorism and its symbiotic relationship with terrorist activities [5, 9–11], there remains a scarcity in understanding the nuanced role of media in shaping national sentiment amidst conflict, particularly within the Israeli context. The literature underscores the media's potent capability to shape public opinion [2–4], amplify terrorist agendas [6, 7, 9, 12], and navigate the complex interplay between reporting responsibilities and national security imperatives [13–15]. However, what emerges as a critical lacuna is an in-depth analysis of how Israeli media, amidst the harrowing backdrop of the Gaza war, managed to recalibrate public trust, foster a sense of unity, and navigate the ethical quandaries posed by war reporting. This study, therefore, seeks to perform an interpretive analysis of the traditional media content illuminating the intricate dynamics of media coverage during the Gaza war, exploring its contributions to national resilience, the strategic manoeuvring between factual reporting and support for national defence and its role in the broader discourse on terrorism and media ethics.

2. Literature review: media at war, coverage of terror incidents, trust in the news media

2.1 Physical terrorism

Physical terrorism is categorised into three distinct types: suicide attacks, lone wolf attacks, and coordinated attacks, based on their impact. Many experts in terrorism studies contend that suicide attacks are currently the most lethal form of terrorism. These attacks are not only cost-effective but also garner significant attention. Mroszczyk concurs, noting that suicide bombings are particularly deadly and adversely affect civilian populations [16]. Presently, terrorist groups are focusing on enhancing the destructive power of suicide bombings while simultaneously striving to lower their operational costs, aiming to increase their visibility and impact.

Some scholars place greater emphasis on coordinated terrorist attacks than on other forms of physical terrorism. Avdan and Webb argue that these attacks have a more profound psychological impact compared to other types of terrorism, making them seem more threatening [17]. Their research suggests that attacks involving simultaneous strikes on multiple targets are perceived as more dangerous than those targeting a single location. Avdan and Webb also highlight that fear is a key aspect of terrorism, and understanding how terrorism induces fear is crucial for recognising its political ramifications. The actions of the Islamic State of Iraq and Syria (ISIS) serve as examples of such coordinated attacks. For instance, in 2015, terrorist incidents occurred in three different countries on the same day, all orchestrated by ISIS. Gilsinan believes these attacks significantly impact civilians' psychology and daily lives as they create a pervasive fear that anyone could potentially be a terrorist [18].

The influence of physical terrorism and its portrayal in the media significantly shapes public opinion. In the aftermath of terrorist incidents, individuals frequently seek out media sources for comprehensive details, trusting their informativeness. The media's role in shaping public understanding of terrorism, highlighted by the coverage of the September 11 attacks, has been pivotal in moulding perceptions.

Some scholars focus on the influence of acts of terror per se. Rubin, Brewin, Greenberg, Hughes, Simpson, and Wessely, for example, highlight that terrorist attacks cause psychological effects on civilians, inducing increased stress and leading to decreased security and behavioural changes [19].

Others, however, research the effects of both physical acts of terrorism and the media. Huff and Kertzer note the challenges in studying public perceptions of violence, emphasising the media's role in framing incidents as terrorism using language tools [20]. Spencer advises careful media language use. He suggests that even simple, seemingly trivial linguistic instruments, such as metaphors, can be used to convey certain meanings cognitively and reduce terrorism-related anxiety [21].

Proximity to terrorist attacks also shapes threat perception, according to Avdan and Webb [17]. The location of attacks and the victims' race and nationality influence how people perceive the threat. The perceived vulnerability to terrorist threats increases when attacks occur nearby and when the victims' identities closely resemble those of the observers.

Yeniçeri and Dönmez try to explain terrorism with 'lay theories'. Their research, based on a poll they conducted in Turkish universities, found that religious terrorism is perceived as more dangerous than ideological or ethnic terrorism [22]. Demirçivi's survey revealed that women are more concerned about terrorism because they tend to follow news regarding the attacks after the incident takes place [23]. Overall, terrorism had a negative influence on the participants' psychological state, which showed in their word choice in describing it: 'fear', 'violence', 'threat', etc.

International surveys echo these findings, showing similar public sentiments. Brouard, Vasilopoulos, and Foucault's study indicate significant shifts in French public opinion post-2015 Paris and 2016 Nice attacks, with some left-wing sympathisers leaning towards right-wing parties and an overall increase in security concerns [24].

2.2 Terrorism and the media

The relationship between terrorism and the media manifests in two principal forms: one is the engagement with traditional mass media, as discussed by Wilkinson [5], and the other is the interaction with social media platforms, as detailed by Dauber et al [25]. The media's quick interpretation and presentation of events enable individuals to easily understand and frame the narrative of terrorist incidents [26]. The way news is presented in the media aids the public in developing their expectations and opinions regarding terrorist events [4]. Given the widespread availability of various forms of mass media today, they undeniably play a significant role in influencing public agendas and shaping societal perceptions [2]. Some researchers believe that the media's impact on public opinion is more substantial than previously assumed. Bruhn [4] and Madhumitha [27] emphasise that the media has played a crucial role in shaping the public's understanding of terrorism, particularly following major incidents such as September 11, 2001, attacks in the US, the London bombings on July 7, 2004, the Madrid train bombings in 2004 and the Oklahoma City bombing in 1995. Ahern et al. found that television coverage, especially of the September 11 attacks and the Oklahoma City bombing, has led to post-traumatic stress disorder and depression

among civilians [28]. Shah and Faiz suggest that terrorist groups aim to gain immediate attention and propagate their message while also demoralising the public and law enforcement agencies [29]. Media coverage of their activities helps them achieve some of these objectives. Wilkinson [5] asserts that such coverage increases terrorist groups' following, a view shared by Burke [6], who notes that media reporting elevates these organisations' profiles. This rise in the popularity of terrorist groups is attributed to the increased media focus on them, as observed by Paust [11].

Nacos further argues that terrorist organisations escalate their violent acts to attract press attention [9]. Terrorists intensify their attacks, following media coverage, viewing it as a means to publicise their actions, beliefs and goals.

This correlation between media coverage of terrorist activities and a surge in terror attacks is further reinforced by Doward [12]. As a result of using the media to promote their agendas, terrorist groups increased the number of casualties from terror attacks around the world from 3387 to 15,396 between 2000 and 2015.

To show exactly how media attention results in more terror attacks, Jetter [7] studied the impact of media coverage on terrorists' suicide attacks. His findings indicate that the media inadvertently provides a platform for terrorist propaganda. Alexander [8] also sees the mass media as a tool for terrorists to spread their propaganda and conduct psychological warfare.

Research indicates that modern terrorist groups use social media, propaganda, fake news and videos for disseminating their ideology, recruiting members, and instilling fear without physical force, such as through an army [30]. By leveraging social media for publicising their acts and exploiting the news media's coverage, these organisations can recruit globally [10, 31]. Najem [10] highlights a mutually beneficial relationship between mass media and terrorist groups, where the media gains viewership from reporting terror attacks, while terrorists use this coverage to amplify their ideology and expand their influence.

2.3 News coverage of domestic conflicts

Research on how the media reports political disputes reveals that the news agencies are deeply affected by the political conditions in their own countries [32]. Additionally, despite globalisation's impact, the range and character of media coverage often reflect the news outlet's ties to its country, be they geographical, political, or cultural [33–38]. Thus, the media's approach to reporting events varies based on whether the conflict is internal, pertaining to their own nation ('ours'), or external, unrelated to their nation ('theirs') [13–15]. This disparity in treatment ultimately challenges the notion of media objectivity.

Studies demonstrate that when a conflict is domestic, media coverage tends to support national foreign policy goals, especially when the national interest is threatened, thereby acting as a source of 'national integration' [39–41] or the unifying force behind government decisions and actions [42, 43]. The so-called national interest is frequently a construct of the government, which is then shaped and propagated by the media. This process often leads the public to adopt and affirm beliefs that align with these constructed interests.

2.4 Trust in news media

A single universally accepted definition of trust in news organisations does not exist. Trust acts as a bridge between awareness and unawareness [44]. In the context

of media, the bedrock of trust stems from past experiences and expectations related to the function of journalism in democracy and its perceived quality [45].

Trust is directed towards an uncertain future, making it intrinsically fraught with risk and ambiguity since the person placing trust (the trustor) lacks control over the one being trusted (the trustee). Consequently, there is a possibility that failing to meet high expectations may result in disappointment [45–53]. Therefore, trust becomes particularly significant in situations where trustors are unable to verify the provided information independently or possess incomplete information. By choosing to trust, individuals do not feel the need to seek out all the details themselves, thereby simplifying complex social interactions and decisions. This is the reason why trust acts as a mechanism that reduces the complexity inherent in social interactions ('social complexity') [52, 54–56].

Trust in news media can be defined as an individual's willingness to be vulnerable to media, anticipating its satisfactory performance and adherence to prevailing societal norms and values, as described by Hanitzsch et al. [47, 48, 57, 58].

Several concepts are associated with trust such as confidence, credibility, scepticism, distrust, and mistrust [59–61]. While trust and confidence are often used interchangeably [62], many scholars differentiate them, noting that trust involves an active decision, unlike confidence [53, 63]. Some argue that true trust in institutions, including the media is not feasible due to the absence of immediate reciprocity, which is one of trust's characteristics. Understandably, this immediate give and take is often absent in the relationship between individuals and large institutions. They suggest that what exists is rather confidence and not trust. Confidence, in this context, implies a belief in the institution's ability to function or act correctly but without mutual interaction [49, 64].

Trust and credibility have also often been used interchangeably or treated as dimensions of each other [51]. Currently, credibility is seen as a more specific concept than trust. It pertains to the evaluation of media content, focusing on the perceived accuracy of information at a specific moment. Unlike trust, credibility does not encompass expectations about future reliability or actions [45, 59, 61].

Studies also deal with terms describing a lack of trust in news media with a prominent example being Tsfati's [65] approach to media scepticism. This approach is defined as 'the feeling that the mainstream media are neither credible nor reliable, that journalists do not live by their professional standards and that the news media get in the way of society rather than help society' [66]. Scholars make a distinction between distrust and mistrust in the media, though the difference is often blurred [67, 68]. Mistrust is seen as systematic and rational doubt equivalent to scepticism [63, 69]. On the other hand, distrust is linked to negative suspicion and cynicism. It represents a strong belief or conviction, often without the need for evidence or rationale, that the subject is not trustworthy [49, 68, 70, 71].

Our research indicates that prior to October 7th, the Israeli media was afflicted with both mistrust and distrust [72]. This is evident as only approximately 20% of the Israeli public expressed confidence in the main media channels according to surveys.

This phenomenon is not unique to Israel but is indicative of a broader, global challenge facing news media in maintaining public support and credibility.

2.5 Summary

Media plays a significant role in shaping public perception of terrorism. There are a number of research directions that explore this relationship. One of them concerns

media coverage and its influence on societal views after major terrorist incidents. As pointed out by Gerbner, Gross, and Bruhn [2–4], terrorist attacks and how the media frames these events have psychological impact. Another one focuses on different forms of physical terrorism and their effect on public psychology. For example, see [16–24]. Other research critically explores the symbiotic relationship between terrorism and media, both traditional and social, highlighting the potential for media coverage to inadvertently support terrorist propaganda, as indicated by Jetter and Alexander [7, 8]. For example, see [2, 4–12, 25–31]. Another area of focus is examining the differences in coverage of external and internal conflicts. For example, see Refs. [13–15, 32–43]. Finally, there are studies that cover the concept of trust in the news media. For example, see Refs. [44–64].

The aim of our current research is to examine the themes presented in traditional media during the early stages of the Gaza war, evaluating their effectiveness in gaining public trust, steering clear of content that might benefit terrorist agendas and supporting Israel's foreign policy objectives. This analysis seeks to unravel the intricate dynamics between media coverage, public perception and trust within the context of terrorism.

3. Methodology

From October 7 to October 28, 2023, the first 3 weeks of the war, the researchers, both individually and jointly, watched broadcasts on Israel's main television channels: Channel 11 (Israel Broadcasting Corporation), Channel 12 (the leading commercial channel in Israel) and Channel 13 (another Israeli commercial private channel) (see Appendix A). Each day, they watched at least 3 hours of broadcast on each channel, covering morning, daytime, early evening and prime-time slots, totalling approximately 200 hours per researcher or about 400 hours combined. They recorded the main themes presented in these broadcasts daily, summarising them at the end of each day and after the observation period, leading to the initial conclusions presented in the following chapter.

4. Results

This chapter delves into the key themes and motifs identified from observing the media coverage.

4.1 Together we will win

Starting at 06:30 on Saturday, October 7, 2023, Israel's established broadcast media, channels 11, 12, and 13, began an extensive coverage of the tragic events of Black Saturday. This coverage of Hamas terrorism and the ensuing war in Gaza was continuous and comprehensive, spanning from 6:30 a.m. to 1 a.m. daily throughout the period under review.

In the wake of Black Saturday, as state institutions, including the police and army in southern Israel, faced a general collapse, the media was the first to regain composure and start functioning effectively. This happened well before the army, police, Shin Bet and other government bodies, many of which struggled to operate properly in the initial days of the conflict, and some continued to face challenges in the weeks that followed.

From the early hours of that Saturday, reporters and broadcasters were on the ground in the area surrounding the Gaza Strip, the epicentre of the Hamas terror. They provided live coverage from there, initiating continuous broadcasts that included news updates, reports and in-studio discussions about the unfolding events (see Appendix A).

Presenters and reporters embarked on an unprecedented professional effort from the first day of broadcasting, continuing throughout the conflict. Their dual objectives were challenging yet crucial: firstly, to provide the Israeli public with reliable, accurate and comprehensive information about the developments on the borders, in the army, on the ground, in communities under attack, within the government and in the health system, including the treatment of abductees and support for residents evacuated from their communities. Secondly, they aimed to address the entire Israeli public, which was considered to be mostly on the home front, but despite being away from the immediate conflict zone, was suffering from continuous missile attacks from Gaza.

The media's effort aimed to stabilise the situation, providing vital civil defence information to the home front. This effort involved supporting, encouraging and strengthening the public spirit while conveying a sense of optimism, unity and collective effort in wartime. From the war's outset, motivational captions were displayed on the screen margins, becoming a key broadcast feature. Channel 11 adopted the slogan 'We are here', Channel 12 used 'Together we will win' and Channel 13 chose 'Strong together'. These expressions were designed to boost viewer morale, foster a sense of solidarity and mutual responsibility and signify the channels' commitment to Israeli society's collective effort against the enemy.

The media undertook the role of unifying and encouraging the people during these challenging times, focusing on the overarching goal of victory. The broadcast media in Israel fully committed itself to the fight against Hamas and to bolster the spirits of those on the home front. This commitment was essential because the impact of war extended beyond those injured, bereaved, or taken hostage; nearly the entire Israeli public faced continuous missile and rocket attacks from Gaza, forcing people to seek refuge in shelters and safe rooms. The enduring and unifying slogan throughout this period was 'Am Yisrael Chai' (The Nation of Israel Lives On). All slogans can be found in Appendix A.

In line with our findings, according to a survey conducted by Yifat research and consulting, there has been a notable increase in the credibility of television channels, with Channel 12 emerging as the most trusted media outlet, experiencing an 11% increase in viewership preference and a 14% increase in trust levels. Conversely, the printed press has seen a significant decline in trust, indicating a shift in the public's media consumption habits and trust allocations. The survey also highlights a decrease in trust towards social networks during the war, with only 31% of respondents expressing trust in the content disseminated through these platforms, a drop of over 20%. Furthermore, the survey reveals that the public's perception of 'Israeli-ness' in media has also undergone changes, with Channel 12 being perceived as the most 'Israeli' media outlet for the first time during the conflict [73].

4.2 Criticism of the government

Most media outlets and reporters conscientiously worked to uphold journalistic ethics as they interpreted them, aiming to serve Israeli society. Their goal was to effectively communicate the events taking place in alignment with their commitment to professional integrity and the interests of their viewers.

From the start, there was indication of a significant failure on the part of state institutions and the government, which resulted in the surprise invasion of Hamas terrorists. Additionally, the reports revealed that these institutions were not operating effectively nor were they responding with the necessary speed and urgency to support those affected.

The reports included candid expressions of citizens' and reporters' frustration, difficulty, pain and despair. They also featured genuine criticism of the government's dysfunction, the Prime Minister's failure to acknowledge his responsibility and the catastrophic failure that precipitated the disaster.

As opposed to the government, members of the defence establishment and the military made statements acknowledging the failure and accepting responsibility for it in the early days of the war.

The Prime Minister's conspicuous refusal to hold himself accountable was broadly criticised across the media. This attitude stood out remarkably, with the notable exception of Channel 14, which is politically aligned with the government.

In the first 2 weeks of broadcasting, there was a notable absence of government representatives, ministers, Knesset members and pro-government journalists. This lack of their presence allowed for extensive criticism and allegations regarding the government's incompetence and significant failures that contributed to the disaster. A major point of criticism centred on the government's pursuit of legal reforms over the past year aimed at weakening the Supreme Court. This agenda faced strong opposition from the nation's liberal and democratic citizens, leading to a concerning neglect of security issues.

From the onset, editors and managers confronted the challenge of dealing with prominent reporters and broadcasters who, in recent years, had been notable supporters of the government in the studios. These individuals saw a significant reduction in their airtime. For instance, on Channel 12 News' popular prime-time show 'Studio Friday', which traditionally allocated considerable space to supporters of the Prime Minister and the government, there was a noticeable shift in the first weeks of the war. The programme became more critical of Netanyahu and his administration. Similarly, on other channels, the general tone in the studios leaned towards criticism of the government. This was coupled with expressions of support for the nation's military, the reserves and the resolute fight against Hamas.

4.3 External censorship and internal censorship

Since the onset of the conflict, media coverage has been characterised by a deliberate and judicious approach: thoughtful and balanced. Avoiding sensationalism and the potential pitfalls of live reporting, the media has exercised restraint, particularly in not disseminating images that could cause distress or inadvertently aid the enemy. This policy has been shown in Wilkinson's study as one of the best in response to terrorism [5]. This cautious strategy stems from lessons learned in previous terrorism-related incidents. While the channel's senior editorial team and reporters had access to a wealth of real-time information, they judiciously chose what to air. Their reporting aimed to be comprehensive, accurate and expansive, adhering to censorship norms without chasing sensationalist exclusives. This approach has been seen as providing sufficient coverage within the bounds of responsible journalism.

Hamas terrorists arrived at the terror campaign equipped with more than traditional armaments; they also utilised body cameras, broadcasting live on social networks. Accompanying these militants were so-called 'reporters' from Gaza who provided real-time updates. Their coverage contained graphics and imagery depicting

harsh violence against Israeli civilians, including the killing and burning of children, women and the elderly. These explicit visuals, which extended to the portrayal of acts such as rape and mutilation, were not broadcast on television but were circulated on platforms, such as Telegram (see examples of Telegram channels in Appendix A).

Israeli broadcasters demonstrated significant responsibility in adhering to the country's military censorship laws. They not only complied fully with these directives but also took extra care to avoid airing content that could potentially aid terrorist groups or enemies, such as Hamas. Additionally, journalists frequently reminded their audience of these censorship practices during their broadcasts (see materials regarding censorship and Dana Weiss and Nir Dvori reports on Channel 12 in Appendix A). This approach was partly to assure the Israeli public, who are deeply concerned about national security and often sceptical about the media's commitment to stringent security standards.

In this media approach, a consensus emerged across all broadcasting channels to refrain from airing videos originating from Hamas, even those that might provide updates on captives in Gaza. This decision was rooted in a commitment to safeguard the public from distressing content and to prevent inadvertently aiding Israel's adversaries. The media, thus, positioned itself as an integral component of the national effort and warfare strategy, prioritising public trust and national security over sensationalism. This strategy underscores the media's role in both informing the public and supporting broader national objectives during times of conflict.

4.4 Competition with the Internet

Channel managers and editorial teams were highly aware that the public's media consumption extended beyond traditional television and institutional sources, increasingly encompassing social networks such as Telegram, TikTok and Twitter (Reference to poll results is provided in Appendix A). Rather than yielding to the often sensationalist and lower standards prevalent on these platforms, they opted for an elevated approach. Their strategy was to enhance the professionalism and reliability of their content. This commitment was aimed at making their broadcasts more suitable for sensitive audiences, including children and adults, as well as the general public, who sought refuge from the distressing videos, rampant rumours and misinformation that typically flood these social networks.

The objective of these efforts is to rebuild and strengthen public trust in the media, a trust that has declined globally in recent years, including in Israel [72]. This task involves navigating through a landscape marked by widespread cynicism and a profound crisis of confidence between the media and its audience. While this challenge is daunting, especially as even the most cautious broadcasters must confront and dispel rumours, their diligent efforts in doing so play a crucial role in regaining and reinforcing the trust of the public in media sources.

The broadcasting channels that were examined exhibited a measured approach, refraining from hastily echoing every rumour, photograph or disturbing video circulating on social networks, such as Telegram and WhatsApp (see Materials regarding censorship and Dana Weiss and Nir Dvori reports on Channel 12 in Appendix A). Frequently, broadcasters and reporters made it a point to communicate openly their policy of caution. They emphasised their commitment to not broadcasting unverified rumours and deliberately avoided showing any extreme images or videos that could potentially be offensive.

In Israel, broadcasting adopted a distinctive approach in response to the Israeli Air Force's operations in Gaza, positioning itself as a refuge from the graphic imagery that

began to pervade international media. Global media outlets were showing widespread destruction, of children being harmed and of women and families becoming refugees. However, in Israel, such images were seldom broadcast. On the occasions they were shown, they were typically framed within the context of being Hamas 'propaganda'. This framing was used to highlight perceived biases in global media coverage and to suggest an unfair portrayal of the events unfolding in the region (see Channel 12 news with Dani Kushmaro and Keren Bezalel, world affairs correspondent, in Appendix A).

Israeli broadcasters widely asserted that certain segments of the Arab and Western media displayed clearly anti-Semitic and hypocritical tendencies in their coverage. They criticised these media outlets for focusing predominantly on the damage and casualties in Gaza while allegedly neglecting to adequately report on the vast acts of terror that were occurring against Israel and the 240 individuals abducted by the Hamas terrorists and taken to Gaza on Black Saturday. This narrative from Israeli broadcasters emphasised a perceived imbalance and unfairness in the international reporting of the conflict.

4.5 A measured and moderate description of death

The channels balanced their broadcasts, avoiding an overwhelming focus on tragedy, instead intertwining narratives of grief with accounts of bravery, resilience and survival (see Programmes dedicated to the topic of heroism in Appendix A). This approach mirrored the 'Holocaust and heroism' motif prevalent in Israel in the discussion of the Holocaust and World War II, where stories of hardship are often accompanied by acts of courage and overcoming. Following each account of a survivor or a bereaved family member, stories highlighting rescue efforts and bravery in adversity were featured, maintaining this thematic balance.

The stories of families, children and women hiding in attics, in safe rooms, and being murdered in cold blood brought to mind in Israel the Holocaust of European Jews during World War II. Hamas was often compared to the Nazis of Germany (see Comparison to Nazi Regime in media coverage in Appendix A). While acknowledging the connection to the Holocaust, the media's stance was clear; the situations were not the same. The emphasis was on the contrast between the past, where Jews were solely victims, and the present, where the Jews have the state and army and can defend themselves. The focus was not just only on death and suffering but also on the themes of resilience and revival that emerged from these events.

The terrible disaster that resulted in 1200 murders and thousands of injuries in a single day left both the media and the entire Israeli public profoundly shocked. Funerals, although numerous across the country, received limited airtime, with only brief mentions, a couple of sentences from heartfelt eulogies, a swift glimpse of the gathering at the cemetery and nothing more. The sheer magnitude of the casualties made it impossible to dedicate individual screens to each victim; instead, screens displayed around 20 to 30 names at once, with a rapid reading of their names. Many people were reported missing, some remained unidentified and a few had no photographs available. The broadcast aimed to pay tribute to the victims and those abducted without turning into a constant stream of funeral coverage and mourning. As emphasised, the focus was on the initial theme, inspiring the Israeli spirit to confront the trauma and work towards resilience and recovery.

4.6 Open studio and continuous broadcasting

Since the war began, the three broadcast channels have maintained continuous open news studios, staffed with reporters, commentators, retired generals and security and military experts. These individuals rotated throughout the extended broadcasting hours. While this open, nonstop discussion format sustained the broadcasts and provided a platform for regular updates, launch and impact reports and supplemented field reports from professional reporters, it quickly revealed its limitations (see Channel 12 in Appendix A).

Most panellists in these studios were older generals and former senior defence officials who relied solely on media reports for information. Their analyses and discussions, based on past experiences and knowledge, often seemed outdated and misaligned with evolving reality and current events. Noticeably, there was a lack of diversity in the voices on air: very few women, intellectuals, academic experts (not previously affiliated with the defence establishment), foreign diplomats, additional journalists, jurists or citizens from other disciplines appeared.

The channels predominantly treated the event as a military one. In the initial weeks of the war, which the study focused on, other critical aspects—political, social, economic, spiritual, ethical, ideological, cultural and geopolitical—were largely overlooked. These aspects were set aside for coverage at a later time.

4.7 Israel Defense Forces (IDF) spokesperson and government spokesmen

From the onset of the campaign, it was evident that neither the government nor the state had an official spokesperson, responsible for updating citizens, explaining the situation, detailing government decisions, offering reassurance and providing instructions to the home front. This absence was filled by several key figures, most notably the leading broadcasters of the television channels, who voluntarily assumed this role. They were accompanied by spokespeople from the Home Front Command who provided civil defence instructions but were unable to present a comprehensive overview of the campaign's objectives, the progress of the conflict or the country's emergency preparedness.

The most prominent figure in this regard became the IDF Spokesperson, Daniel Hagari, a brigadier general in military uniform who delivered daily media briefings on the fighting's developments (see Official IDF Speaker Announcements across channels in Appendix A).

He became the sole official state representative, addressing the public and fielding questions. Concurrently, Prime Minister Benjamin Netanyahu issued a series of unilateral statements in the form of speeches to the nation—a communication pattern he adopted in the first 2 weeks of the war but has changed since. These addresses, lacking media interaction, did not engage with issues that concerned the public at that time.

5. Discussion

The analysis of Israeli news broadcasts during the initial 2 weeks of the Gaza war reveals several key themes and trends that altogether contribute to the overall effort of the media to establish a higher public trust [73] (also see Overcoming the trust crisis in media in Appendix A). Firstly, there is a pronounced alignment with the State of Israel in its conflict with Hamas, coupled with strong support for the Israel

Defense Forces. Besides, the media channels consciously adhere to the constraints of military and self-imposed censorship, striving to create quality material and ensuring the content does not distress viewers and supports the campaign against Hamas. Generally, this trend mirrors past behaviours of the Israeli media during wartime, and it is a phenomenon observed globally [14, 15].

Does this cause an immediate effect on the relationship between the public and media outlets? Based on the recent data summarised above [73], there was, indeed, a significant shift in the Israeli public's trust in various media outlets following the outbreak of the war, with substantial changes observed before and after the conflict. This shift in trust and viewership patterns suggests a complex relationship between them, highlighting the influence of the current conflict events on media credibility and national identity perceptions in Israel. Further, study is required to explain and analyse this shift comprehensively.

In addition to the abovementioned trends, a novel aspect has emerged in the media coverage: supporting the state during war no longer equates to backing the government or the Prime Minister. The media has shown the ability to differentiate between supporting the military, civilians and the state, and voicing significant criticism of the government, the controlling coalition in the Knesset and the Prime Minister. The latter is particularly criticised for his refusal to acknowledge responsibility for the war's outbreak and the tragic event on October 7, where Hamas terrorists killed approximately 1200 civilians in Israel.

The criticism extends beyond the war's mishandling to the Prime Minister's lack of public engagement, avoidance of local media and preference for foreign media interviews in the United States. It also encompasses the perceived failures of various government ministries—Education, Welfare, Housing, Labour and Finance—in addressing the needs of war victims, evacuees, refugees and the families of the fallen and abducted to Gaza (see Appendix A).

This critical stance of the media might also reflect the sentiments of a large part of the Israeli public, which, prior to the war, protested against the government's plans to weaken the Supreme Court's status and power. In criticising the government, the media may be seizing yet another opportunity to regain public trust, aligning with the public's discontent with the government.

Our study shows that the traditional Israeli media leans towards distinguishing its approach from that seen on social media platforms (see Appendix A). It strategically engages itself in a campaign aimed at educating, supporting and safeguarding the Israeli public in the face of terrorism. This choice reflects an understanding of terrorism's primary objective: to sow fear and undermine public morale. Unlike the graphic and often disturbing content circulated on social media, which unflinchingly portrays the atrocities of murder, massacre and rape, Israeli media outlets chose a different path. They opt to concentrate on bolstering the resilience of the Israeli people. This is achieved by fostering a spirit of unity and support for the military, specifically the Israel Defense Forces (IDF) and its spokesperson, while also allowing space for criticism of the government.

By focusing on strengthening the community's resolve and resilience, the media plays a crucial role in mitigating the psychological impact of terrorism [5, 6]. This approach not only helps in maintaining a sense of normalcy and security among the public but also in promoting a collective response to the threats faced by the nation.

According to the recent polls [73], the impact of the Israeli media's strategy on public perception was significant, leading to noticeable shifts in the public's trust towards various news outlets. This suggests that the media's role in shaping public

sentiment and resilience in the face of terrorism is both impactful and recognised by the audience. However, the effectiveness and implications of this media strategy warrant further investigation. Such research would offer valuable insights into the dynamics between media practices and public sentiment during times of national security threats, providing a deeper understanding of the media's power in influencing societal resilience against terrorism.

To sum it up, our observation and analysis show that the Israeli media mobilised for the campaign of informing, supporting and protecting the Israeli public with the understanding that the goal of terrorism is to instil fear and weaken the public's resilience. It saw itself as another arm of the State of Israel in the war against terrorism, in weakening its effect and in strengthening the resilience of Israeli citizens against it. These actions showed immediate response in the shifts of trust of the public towards various news outlets, and yet need to be studied.

The intricate dynamics between national security and media presentation during the Gaza war underscores a pivotal realm of journalistic responsibility and state interest. The Israeli media, in navigating the treacherous waters of war coverage, demonstrated a conscientious balance between the imperative of factual reporting and the ethical considerations tied to national security. The media's strategic decision to emphasise national resilience, while carefully managing the dissemination of sensitive information, showcases an evolved understanding of its role as a guardian of both public interest and national security. This alignment, however, does not detract from the media's critical role in democracy; rather, it highlights the nuanced challenge of reporting in times of crisis. It underscores the importance of a media that, while supportive of national defence, remain vigilant, critical and independent.

In expanding on these connections, future discussions and analyses can further explore the relationship between media practices and national security policies, illuminating the pathways through which media coverage can both reflect and shape the strategic imperatives of state security and public welfare.

6. Limitations of the study and follow-up studies

The current research is qualitative, based solely on the analysts' interpretations of the broadcasts. Given its nature, further research is essential. This includes a more extensive analysis of the number of broadcasts and their specific characteristics, including the airtime not covered in this study, as well as alternative interpretations of these broadcasts. Expanding the scope to include more broadcast and print media and extending the period of study beyond the initial weeks is also crucial. Moreover, a comparative analysis with coverage of the same conflict on international channels in other countries is necessary as this will likely present a markedly different perspective.

Yet another limitation is that this study does not analyse the themes that were not covered by the Israeli media. This acknowledgement highlights the existence of significant aspects of the event and its aftermath that were not addressed in the public discourse, pointing to areas for further investigation.

This study represents a prompt and localised Israeli response to an extraordinary event that garnered exceptional attention both in Israel and globally. Its significance lies in its ability to highlight the event and the nature of media coverage of a major terrorist attack in a country experiencing unprecedented terrorist aggression. This initial analysis serves as a crucial step in understanding the dynamics and implications of media coverage in such critical situations.

7. Summary and conclusion

The study of the findings collected in the first 2 weeks of the war, documents how, in the face of an unprecedented terrorist attack and subsequent conflict in Gaza, the Israeli media, previously nearing a loss of public trust and its status as a guardian of democracy, navigated the complex landscape of war reporting, reasserting its crucial role in a democratic society. Faced with the dual challenge of maintaining journalistic integrity and addressing national security concerns, the media managed to provide the public with timely and accurate news while also handling the collective psychological trauma of the nation.

Notably, the media's efforts went beyond mere reporting; they played a pivotal role in rallying the Israeli spirit, fostering a sense of national unity and sensitively covering the stories of the fallen, wounded, captives and others affected by the events. This nuanced approach underscored the media's commitment to preserving the interests of national security, highlighting its transformation into an entity that not only informed the public but also contributed significantly to the nation's resilience in the face of terror.

Furthermore, the research illuminates the media's strategic pivot towards a more nuanced differentiation between state support and government criticism. While staunchly backing the defence forces and the broader state apparatus in the conflict against Hamas, the media simultaneously cultivated a critical stance towards the government's handling of the crisis, thereby reflecting and potentially shaping public sentiment.

Moreover, the study reveals a significant shift in public trust towards the media, with marked changes in viewership patterns and trust metrics post-conflict. This shift underscores the impact of media practices on national identity perceptions and the credibility of news outlets in crisis situations. It also highlights the potential for further exploration into the dynamics of media influence on public sentiment and national security policies.

In conclusion, by balancing the public's need for information with the collective handling of trauma and maintaining a critical yet supportive stance towards the state, the Israeli media reaffirmed its indispensable role in the fabric of Israeli democracy. As this study shows, the media's actions during the conflict reflect a broader commitment to strengthening societal resilience against terrorism, thus offering valuable lessons for media practices in times of national security threats.

Appendix A. The collection of broadcast channels and media materials

The materials in the collection are taken from the broadcasts aired in the first 2 weeks of the Gaza war, dating between October 7th and October 22nd.

The materials are in Hebrew, and only some of them have English subtitles. In the future research, relevant items should be translated and coded.

The materials are organised in blocks for convenience.

A.1 The official YouTube channels for Israeli broadcasters 11, 12 and 13

Channel 11: https://www.youtube.com/@KAN11
Channel 12: https://www.youtube.com/@israelnews
Channel 13: https://tinyurl.com/2uysa36d

A.2 Slogans adopted by the channels

Slogan 'We are here': https://www.kan.org.il/content/dig/digital/p-11412/

Slogan 'Together we will win': https://www.mako.co.il/tv-special/win_together-articles

Slogan 'Strong Together': https://13tv.co.il/stronger-together/

Slogan The Nation of Israel Lives On: https://www.ynet.co.il/yedioth/article/yokra13647241

A.3 Competition with the Internet and silence of the official media

Emergency provisions: https://www.idi.org.il/articles/51126

On the dominance of the social media: https://www.themarker.com/captain-internet/2023-10-07/ty-article/0000018b-08fe-dc5d-a39f-9efedcc80000

On the elevated Internet ad social media use after the launch of the war: https://www.themarker.com/advertising/2023-11-12/ty-article/0000018b-c321-dea2-a9bf-d3bf22870000

Overcoming the trust crisis in media: Karniel Y, Lavie-Dinur A. War again [Internet]. The Liberal; [cited 2024 Apr 2]. Available from: https://theliberal.co.il/war-again/ (in Hebrew)

A.4 Broadcasts, day by day

- 7.10 https://www.youtube.com/watch?v=KyElYpQ3MUI
- 8.10 https://www.youtube.com/watch?v=q69YrUMn4eE
- 9.10 https://www.youtube.com/watch?v=hYExIh1lsDY
- 10.10 https://www.youtube.com/watch?v=hgQwqYwifVQ
- 11.10 https://www.youtube.com/watch?v=NH169yQHrBc
- 12.10 https://www.youtube.com/watch?v=UcpI4aHQNZA
- 13.10 https://www.youtube.com/watch?v=wH_PlnexEWw
- 14.10 https://www.youtube.com/watch?v=5BOVyiXTUWM
- 15.10 https://www.youtube.com/watch?v=rYAwsYe8Pa8
- 16.10—Special Broadcast https://www.youtube.com/watch?v=ziz9tkBk_v0
- 16.10 https://www.youtube.com/watch?v=A1auuRiC5X4
- 17.10—Special Broadcast https://www.youtube.com/watch?v=rWoq36M-pQY
- 17.10 https://www.youtube.com/watch?v=72vQo-Pf9Z4

- 18.10 https://www.youtube.com/watch?v=WYtEY_CUJ5M
- 19.10—Special Broadcast https://www.youtube.com/watch?v=LBI-WURX8Xw
- 19.10 https://www.youtube.com/watch?v=lv29Qjm0nKc
- 20.10 https://www.youtube.com/watch?v=qXQBLtKMxac
- 21.10—Special Broadcast https://www.youtube.com/watch?v=Qt1ZaViOVPA
- 21.10 https://www.youtube.com/watch?v=oyF9oO111Dk
- 22.10—Special Broadcast https://www.youtube.com/watch?v=lYxqpRg3pPE
- 22.10 https://www.youtube.com/watch?v=Guyz12dGhc8

A.5 Programmes dedicated to the topic of heroism

https://www.youtube.com/watch?v=BBqqzKxqCTQ
https://www.youtube.com/watch?v=faCl3fYtSjY
https://www.youtube.com/watch?v=sF77mb7hQOg
https://www.youtube.com/watch?v=FkDi1gNT8Jw

A.6 Uncensored Telegram channels

https://t.me/Uncensored7_10
https://t.me/massacre7ofoctober

A.7 Samples of criticism towards the PM

https://www.youtube.com/watch?v=2XvXvOOUl4o
https://www.youtube.com/watch?v=fCQaWHoeGXw

A.8 Materials regarding censorship

https://www.themarker.com/advertising/2023-11-15/ty-article/0000018b-ce96-dffa-adef-ee96d3410000
https://www.themarker.com/blogs/2023-10-30/ty-article/.premium/0000018b-7f4a-d51e-a3cb-7f6e374f0000
https://www.maariv.co.il/news/israel/Article-1050713

A.9 Comparison to Nazi Regime in TV coverage

https://fb.watch/rbC7ZKjP-E/

A.10 Official IDF Speaker Announcements across channels

https://www.youtube.com/watch?v=lnUJQNpBCKE

Author details

Yuval Karniel* and Amit Lavie-Dinur
Sammy Ofer School of Communication, Reichman University, Herzliya, Israel

*Address all correspondence to: karniel@krnl.co.il

IntechOpen

References

[1] Lederman J. Battle lines: The American media and the intifada. Philadelphia, Pennsylvania, USA: Orbis. 1993;**37**(1):177. DOI: 10.1016/0030-4387(93)90057-j

[2] Gerbner G, Gross L, Morgan M, Signorielli N, Shanahan J. Growing up with television: Cultivation processes. In: Bryant J, Zillmann D, editors. Media Effects. Mahwah, NJ: Lawrence Erlbaum Associates; 2002. pp. 53-78. DOI: 10.4324/9781410602428-7

[3] Shrum LJ. Cultivation theory: Effects and underlying processes. In: The International Encyclopedia of Media Effects. Hoboken, NJ, USA: Wiley-Blackwell; 8 Mar 2017. pp. 1-12. DOI: 10.1002/9781118783764.wbieme0040

[4] Bruhn DC. News coverage on terrorism: The influence of affect-laden images on information processing [undergraduate thesis]. Enschede, Netherlands: University of Twente; 2009

[5] Wilkinson P. The media and terrorism: A reassessment. Terrorism and Political Violence. 1997;**9**(2):51-64. DOI: 10.1080/09546559708427402

[6] Burke J. There is no silver bullet: ISIS, Al-Qaida and the myths of terrorism. The Guardian. 2015. Available from: https://www.theguardian.com/world/2015/aug/19/isis-al-qaida-myths-terrorism-war-mistakes-9-11

[7] Jetter M. Jetter M. Terrorism and the Media. In: IZA Discussion Paper No. 8497. 2014. DOI: 10.2139/ssrn.2505359

[8] Alexander Y. Terrorism, the media and the police. Journal of International Affairs. 1978;**32**(1):101-113. Available from: http://www.jstor.org/stable/24356774

[9] Nacos BL. Mass-Mediated Terrorism. Lanham, MD: Rowman & Littlefield; 2002. 208 p

[10] Najem T. The symbiotic relationship between the media and terrorism. In: Islamic Military Counter Terrorism Coalition. Riyadh, Saudi Arabia: Naif Arab University for Security Sciences; 2018. Available from: https://imctc.org/UploadedImages/636542881281355269.pdf

[11] Paust JJ. International law and control of the media: Terror, repression and the alternatives. Indiana Law Journal. 1978;**53**(4):Art. 2. Available from: https://www.repository.law.indiana.edu/ilj/vol53/iss4/2

[12] Doward J. Media coverage of terrorism 'leads to further violence'. The Guardian. 2015. Available from: https://www.theguardian.com/media/2015/aug/01/media-coverage-terrorism-further-violence

[13] Cohen A, Adoni H, Nossek H. Television news and the intifada: A comparative study of social conflict. In: Cohen A, Wolfsfeld G, editors. Framing the Intifada: People and Media. Norwood, NJ: Ablex; 1993

[14] Liebes T. Our war/their war: Comparing the intifada and the gulf war on U.S. and Israeli television. Critical Studies in Mass Communication. 1992;**9**(1):44-55. DOI: 10.1080/15295039209366814

[15] Nossek H. Our news and their news. Journalism. 2004;**5**(3):343-368. DOI: 10.1177/1464884904044941

[16] Mroszczyk J. John Mueller and Mark G. Stewart: Chasing ghosts:

The policing of terrorism. Democracy and Security. 2016;**12**(3):219-220. DOI: 10.1080/17419166.2016.1205333

[17] Avdan N, Webb C. The big, the bad, and the dangerous: Public perceptions and terrorism. Dynamics of Asymmetric Conflict. 2018;**11**(1):3-25. DOI: 10.1080/17467586.2017.1414276

[18] Gilsinan K. Terrorist attacks on schools have soared in the past 10 years. The Atlantic. 2014. Available from: https://www.theatlantic.com/international/archive/2014/12/terrorist-attacks-on-schools-have-soared-in-the-past-10-years/383825/

[19] Rubin GJ, Brewin CR, Greenberg N, Hughes JH, Simpson J, Wessely S. Enduring consequences of terrorism: 7-month follow-up survey of reactions to the bombings in London on 7 July 2005. British Journal of Psychiatry. 2007;**190**(4):350-356. DOI: 10.1192/bjp.bp.106.029785

[20] Huff C, Kertzer JD. How the public defines terrorism. American Journal of Political Science. 2017;**62**(1):55-71. DOI: 10.1111/ajps.12329

[21] Spencer A. The social construction of terrorism: Media, metaphors and policy implications. Journal of International Relations and Development. 2012;**15**(3):393-419. DOI: 10.1057/jird.2012.4

[22] Yeniçeri Z, Donmez A. Perception of terrorism and terrorist: How important who holds the gun? Türk Psikoloji Dergisi. 2008;**23**(62):93-107

[23] Demirçivi ER. Metropollerde terörizm algısı: Ankara'da bir uygulama [Perception of terrorism in metropolises: A case study in Ankara] [MSc diss.]. Ankara, Turkey: Turkish Military Academy, National Defence University, Department of Security Sciences; 2015

[24] Brouard S, Vasilopoulos P, Foucault M. How terrorism affects political attitudes: France in the aftermath of the 2015-2016 attacks. West European Politics. 2018;**41**(5):1073-1099. DOI: 10.1080/01402382.2018.1429752

[25] Dauber CE, Robinson MD, Baslious JJ, Blair AG. Call of Duty: Jihad-How the video game motif has migrated downstream from Islamic State propaganda videos. Perspectives on Terrorism. 2019;**13**(3):17. Available from: https://www.jstor.org/stable/26578183

[26] Norris P, Kern M, Just MR. Framing Terrorism: Understanding Terrorist Threats and Mass Media. London: Routledge; 2003

[27] Madhumitha DS. Terrorism in Media Land. International Journal of Law Management & Humanities. 2019;**2**(4):155-165. Available from: https://www.ijlmh.com/paper/terrorism-in-media-land/

[28] Ahern J, Galea S, Resnick H, Kilpatrick D, Bucuvalas M, Gold J, et al. Television images and psychological symptoms after the September 11 terrorist attacks. Psychiatry: Interpersonal and Biological Processes. 2002;**65**(4):289-300. DOI: 10.1521/psyc.65.4.289.20240

[29] Shah MH, Faiz M. Terrorism and foreign direct investment: An empirical analysis of SAARC countries. In: MPRA Paper No. 82008. Munich: University Library of Munich, Germany; 2015. Available from: https://mpra.ub.uni-muenchen.de/82008/

[30] Soderlund WC, Najem TP, Roberts B. Libya, 2011: Reconstruction of a failed R2P intervention. In: Paper Presented at: Meeting of the Canadian Political Science Association. Toronto, ON: Ryerson University; 2017. Available from: https://cpsa-acsp.ca/documents/

conference/2017/Soderlund-Najem-Roberts.pdf

[31] Khosrokhavar F. Inside Jihadism: Under-standing Jihadi Movements Worldwide. New York, NY, USA: Routledge; Dec 2015. DOI: 10.4324/9781315633930. ISBN: 9781317257523. Available from: https://www.taylorfrancis.com/books/9781315633930

[32] Oliver PE, Maney GM. Political process and local newspaper coverage of protest events: From selection bias to triadic interaction. The American Journal of Sociology. 2000;**106**:463-505

[33] Chang TK, Lee JW. Factors affecting gatekeepers' selection of foreign news: A National Survey of Newspaper Editors. Journalism Quarterly. 1992;**69**(3):554-561. DOI: 10.1177/107769909206900303

[34] De Vreese H, Peter J, Holli AC. Framing politics at the launch of the euro: A cross-national comparative study of frames in the news. Political Communication. 2001;**18**(2):107-122. DOI: 10.1080/105846001750322934

[35] Rosengren KE. International news: Methods, data and theory. Journal of Peace Research. 1974;**11**(2):145-156. DOI: 10.1177/002234337401100208

[36] Sreberny A, Stevenson R. Comparative analysis of international news flow: An example of global media monitoring. In: Nordenstreng K, Griffin MS, editors. International Media Monitoring. Cresskill, NJ: Hampton Press; 1999

[37] Westerståhl J, Johansson F. Foreign news: News values and ideologies. European Journal of Communication. 1994;**9**(1):71-89. DOI: 10.1177/0267323194009001004

[38] Wu H. Systemic determinants of international news coverage: A comparison of 38 countries. Journal of Communication. 2000;**50**(2):110-130. DOI: 10.1093/joc/50.2.110

[39] Bloch-Elkon Y. Studying the media, public opinion, and foreign policy in international crises: The United States and the Bosnian Crisis, 1992—1995. Harvard International Journal of Press/Politics. 2007;**12**(4):20-51. DOI: 10.1177/1081180x07307184

[40] Paletz DL. The Media in American Politics: Contents and Consequences. 2nd ed. New York: Longman; 2002

[41] Schudson M. What's unusual about covering politics as usual. In: Journalism After September 11. New York, NY, USA: Routledge; pp. 36-47. DOI: 10.4324/9780203218136_chapter_2

[42] Rivenburgh N. Social identification and media coverage of foreign relations. In: Malek A, editor. News Media & Foreign Relations. Norwood, NJ: Ablex; 1996

[43] Waisbord S. Journalism, risk, and patriotism. In: Zelizer B, Allan S, editors. Journalism After September 11. New York: Routledge; 2002

[44] Vanacker B, Belmas G. Trust and the economics of news. Journal of Mass Media Ethics. 2009;**24**(2-3):110-126. DOI: 10.1080/08900520902885277

[45] Prochazka F, Schweiger W. How to measure generalized trust in news Media? An adaptation and test of scales. Communication Methods and Measures. 2018;**13**(1):26-42. DOI: 10.1080/19312458.2018.1506021

[46] Blöbaum B. Trust and journalism in a digital environment. In: Reuters Institute for the Study of Journalism

(RISJ) Working Papers. Oxford, United Kingdom: University of Oxford; 2014

[47] Grosser KM. Trust in online journalism. Digital Journalism. 2016;**4**(8):1036-1057. DOI: 10.1080/21670811.2015.1127174

[48] Hanitzsch T, Van Dalen A, Steindl N. Caught in the Nexus: A comparative and longitudinal analysis of public trust in the press. The International Journal of Press/Politics. 2017;**23**(1):3-23. DOI: 10.1177/1940161217740695

[49] Hardin R. Trust. Key Concepts. Cambridge, UK: Polity Press; 2006

[50] Jackob N. Gesehen, Gelesen—Geglaubt?: Warum die Medien Nicht die Wirklichkeit Abbilden und die Menschen Ihnen Dennoch Vertrauen. München: Olzog; 2012

[51] Kohring M, Matthes J. Trust in news media. Communication Research. 2007;**34**(2):231-252. DOI: 10.1177/0093650206298071

[52] Luhmann N. Trust and Power. In: King M, Morgner C, editors. Davis H, Raffan J, Rooney K, translators. Reprint ed. Cambridge, UK: Polity Press; 2017

[53] Sztompka P. Trust: A Sociological Theory. Cambridge: Cambridge University Press; 1999

[54] Barber B. The Logic and Limits of Trust. New Brunswick: Rutgers University Press; 1983

[55] Bierhoff HW. Politisches vertrauen. Verschiedene dimensionen, verschiedene ebenen der betrachtung, Political trust: Different dimensions, different levels of consideration. In: Schmalz-Bruns R, Zintl R, editors. Politisches Vertrauen. Soziale Grundlagen Reflexiver Kooperation, Political Trust. Social Foundations of Reflexive Cooperation. Baden-Baden: Nomos; 2002. pp. 241-254

[56] Offe C. Political liberalism, group rights, and the politics of fear and trust. Studies in East European Thought. 2001;**53**(3):167-182. Available from: https://www.jstor.org/stable/20099760

[57] Dernbach B. Was schwarz auf weiß gedruckt ist… Vertrauen in Journalismus, Medien und Journalisten. In: Vertrauen und Glaubwürdigkeit. Wiesbaden, Germany: Verlag für Sozialwissenschaften; 2005. pp. 135-154. DOI: 10.1007/978-3-322-80505-8_8

[58] Prochazka F. Vertrauen in journalismus. In: Vertrauen in Journalismus unter Online-Bedingungen. Wiesbaden, Germany: Springer VS; 2020. pp. 33-55. DOI: 10.1007/978-3-658-30227-6_3

[59] Engelke KM, Hase V, Wintterlin F. On measuring trust and distrust in journalism: Reflection of the status quo and suggestions for the road ahead. Journal of Trust Research. 2019;**9**(1):66-86. DOI: 10.1080/21515581.2019.1588741

[60] Fisher C. The trouble with 'trust' in news media. Communication Research and Practice. 2016;**2**(4):451-465. DOI: 10.1080/22041451.2016.1261251

[61] van Dalen A. Journalism, trust, and credibility. In: The Handbook of Journalism Studies. New York, NY, USA: Routledge; 20 Jun 2019. pp. 356-371. DOI: 10.4324/9781315167497-23

[62] Cook TE, Gronke P. The dimensions of institutional trust: How distinct is public confidence in the media? In: Proceedings of the 59th Annual Conference of the Midwest Political Science Association, Chicago, IL, USA. Bloomington, Indiana, USA:

Midwest Political Science Association; 2001

[63] Norris P. The conceptual framework of political support. In: Van der Meer T, Zmerli S, editors. Handbook on Political Trust. Cheltenham, UK: Edward Elgar; 2017. pp. 18-32. DOI: 10.1080/21515581.2017.1364481

[64] Levi M. A state of trust. In: Braithwaite V, Levi M, editors. Trust and Governance. New York: Sage; 1998. pp. 77-101. Available from: https://static1.squarespace.com/static/5c05f8595cfd7901fc57139d/t/5c871e3e4e17b645c8b1f791/1552358991376/vb_ml_98_trust+and+governance.pdf

[65] Tsfati Y. Media skepticism and climate of opinion perception. International Journal of Public Opinion Research. 2003;**15**(1):65-82. DOI: 10.1093/ijpor/15.1.65

[66] Tsfati Y, Cappella JN. Do people watch what they do not trust? Communication Research. 2003;**30**(5):504-529. DOI: 10.1177/0093650203253371

[67] Ladd JM. The role of media distrust in partisan voting. Political Behavior. 2010;**32**(4):567-585. DOI: 10.1007/s11109-010-9123-z

[68] McKnight HD, Chervany NL. Trust and distrust definitions: One bite at a time. In: Lecture Notes in Computer Science. Berlin, Germany: Springer; 2001. pp. 27-54. DOI: 10.1007/3-540-45547-7_3

[69] van der Meer TWG, Zmerli S. The deeply rooted concern with political trust. In: Handbook on Political Trust. Cheltenham, UK: Edward Elgar Publishing; 27 Jan 2017. DOI: 10.4337/9781782545118.00010

[70] Citrin J, Stoker L. Political trust in a cynical age. Annual Review of Political Science. 2018;**21**(1):49-70. DOI: 10.1146/annurev-polisci-050316-092550

[71] van der Meer TWG. Democratic input, macroeconomic output and political trust. In: Handbook on Political Trust. Cheltenham, UK: Edward Elgar Publishing; 27 Jan 2017. DOI: 10.4337/9781782545118.00028

[72] Karniel Y, Lavie-Dinur A. A Loss of Trust, Reflected in the Media and Politics. Tel-Aviv, Israel: Resling Publishing; 2022. [in Hebrew]

[73] Walla! Ratings are Nice, but a Major Study Reveals Who the Public Trusts in War [in Hebrew]. 2023. Available from: https://b.walla.co.il/item/3621234

Chapter 5

Cybercrimes as a Potential Threat to National Security: The Case of Kosovo

Haki Demolli

Abstract

The focus of the chapter is cybercrime and the danger it poses to the national security of Kosovo. In order to present the situation of this problem in Kosovo, the author concentrates on cyberattack cases in which the national security of Kosovo has concentrates on cyberattack cases in which the national security of Kosovo has been threatened during the last few years. Kosovo's national security is being attacked by various forms of cybercrime, which are mostly carried out by cybercriminal groups from countries that oppose Kosovo's independence, such as Serbia, Russia, Bosnia, and Herzegovina. The author analyzes the volume and dynamics of cybercrime offenses committed in Kosovo over the last 8 years. Analytical studies are conducted on legislative measures. Among such measures is the cyber security legislation, which in Kosovo is sufficient and meets the needs of its citizens, as it is in accordance with aquis communiter, legal standards, and other legal acts of the EU. The various state mechanisms that Kosovo has established during the past decade, which are solely dedicated to preventing and combating cybercrimes in this small European state, have also been addressed. The new types of cybercrimes pose a significant challenge for Kosovo, which is constantly evolving, affecting various computer systems and social values, including national security.

Keywords: cybercrime, national security, cyberattacks, computer system, Kosovo, cybersecurity, challenge

1. Introduction

In Kosovo, the increase in the use of computers and Internet networks in recent decades has directly affected the improvement of the quality of life of its citizens and enabled the realization of various economic benefits, especially through rapid relative growth rates of cyber-producing sectors [1].

According to the European Union Statistical Office (Eurostat), from 2017 until 2023, the percentage of families with access to the Internet in Kosovo has continuously increased. Now, only 1.4% of families are without Internet access [2]. The percentage of families in Kosovo, 98.6 that have access to the Internet is greater than the average in the European Union, which is 92.4. Last year, the main Internet users were

people between 16 and 34 years [2]. Over the years, those over 65 have had the lowest Internet usage in the country [2].

These developments, particularly the fact that the vast majority of services in Kosovo are performed online through digital networks, have made Kosovo an extremely vulnerable country to cyberattacks. Cyberattacks against such digital services have an impact on the privacy of the citizens of Kosovo, as well as on the economy, state security, and societal peace in general.

The Kosovar Center for Security Studies (KCSS) suggests that cybersecurity attacks in Kosovo are directed toward the state computer network system, user accounts, the financial system, websites, and the private sector [1]. Due to Kosovo's unstable relationship with Serbia and lack of normalization, cyberattacks through disinformation campaigns can result in interethnic incidents and violence and endanger national security. Given the risks that cyberattacks create for the economy and state security, Kosovo has taken various measures and actions, as well as established certain mechanisms to prevent and combat cybercrimes.

In the framework of these measures, among the most important are the legislative ones, which regulate the protection of numerous areas that are vulnerable to cybercrimes, carried out in a network that has as its objective or as a way of carrying out the crime, the misuse of computer systems and computer data. The areas that are protected from cybercrime can belong to private businesses, state institutions, industries, economies, national security, or personal actions of ordinary citizens (e.g., child pornography). Then, it regulates and protects electronic communication between different subjects, whether natural or legal persons, with a focus on protecting the rights of individuals to personal data and, in particular, the right to privacy. So, it has created the conditions for the country's institutions to invest in building security capacities in the field of computer technology. Therefore, the focus of this chapter is on cybercrimes in Kosovo, as well as its measures and mechanisms to combat them.

2. Cyberattacks against national security in Kosovo

Cybercrime, as a relatively new phenomenon, is defined in criminal legal doctrine as a crime where computers are used as tools to commit an offense, and the primary targets are computers and computer systems [3].

There are generally two main types of cybercrime: (a) cybercrime that in one way or another is related to "traditional" forms of crime, which have evolved by transferring to the cyber sphere, such as financial offenses, then criminal offenses that affect the safety of children and young people, including terrorism, and (b) the so-called high-tech crime, which is the advanced form of cybercrime, targets computer hardware and software as its main targets of sophisticated attacks [4].

Cybercrime experts emphasize that the motive for committing cyberattacks determines the different types of cyberattacks, which can be classified as cybercrimes motivated by revenge, curiosity, financial gain, espionage, jeopardizing national security, and terrorism [1]. In Kosovo, while cyberattacks with a nature of financial gain and curiosity have been carried out by local criminals, the majority of the attacks on national security have been perpetrated by hackers from countries that oppose Kosovo's independence. In certain periods, Kosovo has had a tendency to receive attacks from the Serbian state, China, Russia, and other countries within this political bloc. Fortunately, these efforts have not caused any significant damage or consequences for the state institutions of Kosovo. An attack of this nature was registered

at the beginning of December 2018, targeting the electronic communication network of the Ministry of Foreign Affairs (MFA) of Kosovo, which resulted in the complete blocking of Kosovo's embassies in the capitals of the different states in official emails. According to Kosovar investigators, the cyberattack lasted for over 24 hours. It was carried out by Serbia, Bosnia and Herzegovina, and North Macedonia. While the representatives of the Ministry of Foreign Affairs of Kosovo (MFAK), stated that "we do not know if they are sponsored by the official Belgrade regarding those who ordered the attack, but we are aware that they are coming from there, and this poses a major threat to Kosovo" [5]. In addition to the MFAK, attacks of this kind have targeted the Ministry of Internal Affairs of Kosovo (MIAK) in 2018 [1]. Cyberattacks against Kosovo institutions occurred in 2021 and 2022 as well. The government's decision on car plate reciprocity on September 20, 2021, is a clear illustration of how foreign malignant influences can have a negative effect on the national security of Kosovo.

Following this decision on car plates, propaganda, disinformation, and fake news from Serbia were spread in the northern municipalities of Kosovo aimed at escalating the situation on the ground, in majority-Serbian communities, stoking fears that the Kosovo Security Forces would enter these majority-Serbian areas [1]. However, in close coordination with international allies, the Kosovo government successfully coordinated all national security mechanisms, preventing the situation from escalating on the ground. This government decision was followed by the highest amount of disinformation and misinformation in the digital space throughout the year, as reported by an organization that monitors online portals [6]. The aforementioned type of cybercrime used against Kosovo's national security is known as "computer disinformation," which, according to the "US Department represents one of the most important and widespread weapons of the Kremlin" [6]. According to a local study, "Kosovo is vulnerable to misinformation and malicious external influences, especially in the media sphere" [6]. One of the reasons for Kosovo's high vulnerability to this type of cybercrime is that over 40% of Kosovo citizens do not verify the information they receive online at all, while only 16% of them check the source of the information [7].

To such cyberattacks, Kosovo's prime minister Albin Kurti reacted himself. He pointed out in September 2023 that Russia and its allies are frequently using disinformation and other malicious behavior in the cyber field as a mechanism, for interfering in the process of dialog and normalizing relations between Kosovo and Serbia [8].

At the beginning of 2022, cyberattacks again targeted the computer systems of the Ministry of Internal Affairs of Kosovo [9]. These attacks were an additional reason for Kosovo's National Cyber Security Council (NCSC) to conduct a comprehensive analysis of the state of cybersecurity and the degree of risk of state institutions, concluding that because they operate in the same cyberspace as other parts of the world, it is expected that they face the same risks [9].

The NCSC claims that Russian hackers from the "KILLNET" group are constantly targeting state institutions. The Ministry of Internal Affairs of Kosovo (MIAK) has been targeted by cyberattacks even in April 2022, as confirmed by its officials through a statement; it was emphasized that "we have had 'Phishing' cyberattacks, but not we have had any cyberattacks that have compromised the infrastructure and we have not suffered any damage from those attacks, although 'Phishing' attacks are frequent" [10]. The "Phishing" type of cyberattack is a form of "social engineering" that aims to steal credentials. With "Phishing" attacks, the victim is tricked into providing their credentials through emails so that the email is professionally modified and sent to officials working in a particular state institution [11]. These emails look very innocent as if they were sent by a friend, a government official, a public institution, a bank,

etc. So, reliable institutions [1]. The victims assume they are on a legitimate site, but in reality, they are on a fraudulent site [12]. Usually, in these emails, there are one or more links or some documents that look safe and in which the victim registers, for example, by giving their email and password [1]; unfortunately, in such cases, the victim gave the email and password to fraudsters/hackers, who aimed to steal credentials, which then would be used for their criminal purposes [12].

The Ministry of Internal Affairs has confirmed that during April 2023, the websites of the three most important institutions of Kosovo, including the Presidency, the Prime Minister's Office and the Prosecutor's Office of Kosovo, were the target of a cyberattack. The type of cyberattack used was Distributed Denial of Service (DDoS). The DDoS attacks affect the availability of web services for an undefined period of time, causing fraudulent requests to flood the company's servers, denying requests from legitimate users and generating economic losses due to rendered services that are unavailable [13]. As a result of this cyberattack, the websites of the Prime Minister's Office, the Presidency, and the State Prosecutor's Office have been out of order from time to time during the attack [14]. An online group called "Anonymous Albania" has taken on the responsibility for these attacks, while the attacks were conducted as a demonstration against the lack of respect for workers' rights and the inadequate response to the 11-year-old girl's rape in Kosovo [1].

In recent years, cybercrime has also appeared in Kosovo as a threat to institutions with bomb explosions, as were the cases with the International Airport of Pristina (several times in June 2022, February 2023, April 2023, etc.), then the University of Prishtina (July 2022), "Xhevdet Doda" Gymnasium in Prishtina (May 2022), the "Gate" discotheque in Prishtina (November 28, 2023), etc., upon receiving emails, the Kosovo Police went to the locations where there were supposed to be bomb attacks, but thankfully they were false alarms.

In addition to the aforementioned cyberattacks, Kosovo has also been afflicted with cybercrimes, which are foreseen as the criminal offense of Unauthorized access to computer systems (UACS) Article 327 of the Criminal Code of Kosovo (CCK) and Infringing privacy in correspondence and computer databases (IPCCD) Article 199 of CCK).

Under Article 327 of the CCK, it is determined that a person commits the criminal offense of Unauthorized access to computer systems if the person does so without authorization and with the intent to obtain an unlawful material benefit for themselves or another person or to cause damage to another person, alters, publishes, deletes, suppresses or destroys computer data or programs or in any other way intrudes into another's computer system [15].

According to the provisions of Article 199 of the CCK, the criminal offense of infringing privacy in correspondence and computer databases is committed by the person who, without authorization, intervenes in the computer database of another person, respectively, the person who without authorization opens the person's consignment (shipment) or electronic communication other, or in any other way uses that data or violates the confidentiality of such materials or without authorization retains, hides, destroys or delivers to another person such paper or electronic communication [16].

Based on the statistics of the Kosovo Judicial Council (KJC) [17], a total of 111 cybercrime criminal offenses were registered in Kosovo between January 2017 and October 2023 (see **Table 1**).

Table 1 shows that between January 2017 and October 2023 (almost 8 years), of the 111 criminal acts of cybercrime committed in Kosovo, 84 or 75.5% were of the

Criminal offenses	2017	2018	2019	2020	2021	2022	2023	In total	Percentage
UACS	11	17	11	10	09	20	06	84	75.5%
IPCCD	04	03	04	05	03	06	02	27	24.5%
	15	20	15	15	12	26	08	111	
	13.5%	18%	13.5%	13.5%	10.8%	23.4%	7.2%		100%

Table 1.
The volume and dynamics of cybercrime offenses registered in Kosovo courts (according to the KJC) between January 2017 and October 2023.

type "unauthorized access to computer systems," while 27 or 24.4% criminal offense were "infringement of confidentiality of correspondence and computer databases."

Looking at the dynamics of such criminal offenses committed during the eight-year period, it can be concluded that, almost in each year of the study period, approximately 15 such offenses (or about 13%) were committed, with the exception of the year 2018 when 20 such crimes were committed (or 18%) and in 2022 the largest number, with a total of 26 (or 23.4%).

In addition to the data on the volume and dynamics of cybercrimes, for the purposes of this paper, some data (not for all criminal cases) related to the gender of the perpetrators and the types of criminal sanctions imposed on them have been provided. Thus, from the total of 111 criminal offenses registered, the data on the gender of 48 of their perpetrators has been provided, of which it can be seen that 39 or 81.25% of them were male, while 9 or 18.75% perpetrators were female. This fact shows that Kosovo women are more likely to participate in cybercrimes (with 18.75%) than in the commission of crimes in general, with 4% in 2013 (573 female perpetrators and 14.473 male perpetrators); with 4% in 2014 (743 female perpetrators and 16.747 male perpetrators), respectively, with 5% in 2015 (769 female perpetrators and 15.755 male perpetrators) [18].

As for the type of criminal sanctions imposed on cybercrime perpetrators in Kosovo, data has been provided for 19 perpetrators, which are presented in **Table 2**.

From **Table 2**, it can be seen that out of 19 perpetrators of cybercrimes, 8 or 42% of them were sentenced to a conditional sentence, then 6 or 31% of them were sentenced to a fine, while only 5 or 25% of them were punished with imprisonment. Given that 73% of cybercrime perpetrators were sentenced to a conditional sentence and a fine, punishments that mainly affect the material values of the perpetrator, it can be concluded that the courts in Kosovo are lenient in their approach to punishing the perpetrators of these crimes. However, only a quarter of perpetrators are sentenced to imprisonment, which is regarded as one of the most severe punishments in

Type of punishment	Conditional sentence	Punishment with a fine	Imprisonment sentence and fine	Imprisonment sentence	In total
Criminal files	08	06	03	02	19
Percentage	42%	31%	15%	10.5%	100%

Table 2.
The types of criminal sanctions imposed by the courts of Kosovo for cybercrime perpetrators (for 19 cases, data has been provided) between January 2017 and October 2023.

contemporary criminal legislation through which the perpetrator is deprived of one of the most precious personal values, which is freedom.

3. Kosovo's risks and challenges in combating cybercrimes

Kosovo, as a country that came out of the war two and a half decades ago, has not developed its industry. This fact has made this area (industry) not a target of cybercrimes, so in a way, it has protected it from this type of crime. As an integral and active member of the international community, Kosovo is in the process of digitizing all its services, activities, business spheres, and every aspect of the life of its citizens. In accelerating this process, the COVID-19 pandemic has served as an important catalyst (the isolation of Kosovo citizens began in March 2020 and has continued throughout 2021), during which period many institutions and businesses in Kosovo switched from the physical system of services to the digital system, circumstances that have increased the interest of hackers and the risk of cyberattacks.

In addition to the digitalization of industrial, commercial, and economic services, it is currently developing the digitalization of state institutions, which process data for nearly 1.7 million citizens responsible for protecting and providing security of their customers' numerous data. Such developments have made (will make) state, administrative, business, commercial, industrial, and other services accessible to every citizen in the world; simply, anyone from any corner of the world can have access to Kosovo's digital platforms, not only to assess the quality of these services but also to identify their weaknesses and take advantage of the opportunity to hack or attack them. So simply these services have become and day by day are becoming even more vulnerable to cyberattacks.

The Kosovar authorities and society as a whole are cognizant of the increasing risks from cybercrimes, so they are constantly taking various actions, measures, plans, and strategies to prevent and successfully fight against cybercrimes. Such efforts by the Kosovar authorities are encountering difficulties and challenges of various natures, which can generally be divided into two groups.

The challenges faced by Kosovo's state institutions in building cyber security capacities, such as the lack of human resources for this type of profile as well as the unsatisfactory stimulation for information technology professionals during the time of exceptional competition with the private sector is a problem that belongs to the first group [19].

This challenge is of global nature therefore Brett Callow, a Canadian analyst at the cybersecurity group Emsisoft, rightly says that cybersecurity experts are in short supply. They go where the money is, so they usually not in government institutions; this fact creates the impression that "local governments seem to have the weakest systems" [20].

Another challenge is that the justice system in Kosovo, particularly the courts, are not professionally prepared to properly handle cybercrime cases, because for Kosovo judges and prosecutors, this field remains largely unknown [1]. Therefore, it is rightly emphasized in a report to the Commission of the European Parliament that Kosovo needs to address the issue of the insufficient availability of cybercrime training for newly appointed judges, prosecutors, and those who handle electronic evidence [1].

The decentralization of computer systems in Kosovo's institutions is another challenge, which means that they do not have control or supervision over each other's data, so they do not have such policies in the cyber sector, which determines whether data is to be transferred from one system to another or from one institution to another; specifically, the state applications of the Tax Agency of Kosovo, do not

exchange information with the Central Bank of Kosovo. This lack of coordination can affect the security aspect of the computer systems of such institutions [21].

Another challenge of this group is the lack of harmonization between different laws, strategies, and other acts in this field. Kosovo has many laws, such as the law on national security, the strategy for national defense and security, the law on telecommunications, and the law on critical infrastructure, which have poor coordination and harmonization among themselves. While cyber security requires harmonization of all laws to respond appropriately to cyberattacks.

There are challenges in the second group that are related to the characteristics or types of cyberattacks. One of the main characteristics of cybercrime is the dynamic evolution of its types. There is no doubt that cybercrime in this direction (plane) is more dynamic than all other forms of contemporary criminality. The evolution of cybercrimes is primarily related to the rise of new technologies, such as artificial intelligence, which has enabled attackers to become more sophisticated in their methods. It is crucial for businesses to stay current with the latest threats, as cybercriminals constantly evolve their tactics. Cybercriminals make use of fileless attacks, which leave no marks on the system, and supply chain attacks, in which they target third-party vendors to gain access to a network [22].

Building the capacity to successfully combat existing types of cybercrimes as well as new types that might emerge against national security, poses another challenge for Kosovo. It is well-known that human society is currently facing more than 50 types of cyberattacks [23]. Given the dynamics of the appearance of such crimes over the past 15 years, during which it is evident that a new type has appeared every 2 years, it is expected that in the coming years, new types of cybercrime will emerge, with which the Kosovar authorities will have to contend.

According to NordLayer, the number of Advanced Persistent Threats (APTs) increased significantly between 2009 and 2012, which are sophisticated attacks designed to steal data from a specific target [24]. Finally, during 2022–2024, another new form of cybercrime emerged, which is manifested by "the creation of realistic videos or audio recordings that can be used to spread misinformation or conduct social engineering attacks." These videos are created by deep fake technology. On the other hand, synthetic identity fraud involves creating fake identities using both real and fake information [24].

What will be the new types of cybercrime that will endanger Kosovo's national security from 2024 onwards? This represents a challenge for this country.

4. Cybercrime in Kosovo's legislation

The Republic of Kosovo is dealing with challenges, risks, and problems related to cybercrime, so it has approved laws and other legal provisions to tackle and successfully combat this phenomenon. There is no doubt that one of the most important laws that defines and sanctions criminal offenses related to cybercrime is the Criminal Code of Kosovo (CCK), which, besides the two criminal offenses of Infringing privacy in correspondence and computer databases (Article 199) and Unauthorized access to computer systems, Article 327 (highlighted above in this paper), as offenses of this nature has also foreseen Avoiding technological measures (Article 291), Identity theft and access equipment (Article 336), etc.

The CCK also contains other criminal offenses that can either be committed in the form of cybercrimes or their commission (methods or means) depending on the use

of an Internet network or a computer, such as the criminal offense of Inciting discord and impatience (Article 141), and the criminal offense of causing general danger (Article 356).

In addition to the provisions of the CCK, Kosovo also regulates cybercrime through other laws, including (1) Law on Prevention and Fight of Cyber Crime (July 2010), (2) Law on Electronic Communications (2012), and (3) Law on Cyber Security (February 2023).

4.1 Law on Prevention and Fight of the Cyber Crime 2010

Law on Prevention and Fight of Cyber Crime is the first law of this nature that Kosovo has ever approved. The law defines a preventive package against cybercrime, which includes the development of cyber policies, awareness campaigns, the development of minimum practices and standards for cybersecurity by authorities and competent public institutions in the field of cyber services, etc. [25].

Determining the scope of the law is done through the definition of basic expressions used to describe this phenomenon, such as "cyber crime," "computer system," "computer program," and "interception." Upon examination of the definition of cybercrime, it becomes evident that three basic requirements must be fulfilled for its existence. First, the act of committing, which may be considered "criminal activity in the form of misuse," then the defense facilities of the criminal offense are "networks or computer systems," and finally, the object of the attack is "computer data."

Given the sensitivity of computer systems, as well as the information transferred through them, including personal data, it is required by law to ensure that human rights are observed and personal information is safeguarded [25], during the development of different procedures.

The law also defines a certain number of criminal offenses of a cyber nature, highlighting their nature and the actions taken to commit them, their aggravated forms, and the criminal sanctions that can be imposed on their perpetrators. To prevent cybercrimes under this law, initial consideration is given to the confidentiality, integrity, and availability of computer system data (Article 9).

Computer data encompasses any form of facts, information, or ideas that are appropriate for processing in a computer system, including a program capable of enabling a computer system to perform a specific function [26]. Under the law, a person who illegally accesses computer systems and accesses such data commits a criminal offense for which he/she can be sentenced to up to 3 years in prison. In addition to illegal access to computer systems, this law also defines a criminal offense as the unauthorized interception and transfer of computer data or its limitation. Modifying, paying back, destroying, or limiting computer data can be classified as criminal offenses for unauthorized transfer.

The law considers as the criminal offense also the obstruction of the functioning of computer systems, then causing loss of property through computer systems, child pornography through computer systems, and other computer-related criminal acts (Article 14) [25] that can be carried out in the form of information entry, amendment or deletion without authorization of computer data, etc.

In addition, the law has regulated the procedure for investigating and criminally prosecuting cybercrime perpetrators, and specific measures have been established to preserve and safeguard the data that was attacked by these crimes.

Cybercrime can cause damage worth billions of dollars within a year [27]. It is an "elusive phenomenon," and as a result, combating it is not simple, primarily because

it develops in a virtual way, which means that there is no material evidence behind it [27]. As a specific procedural measure, the law defines "the storage of computer data" that may be ordered by the prosecutor during investigations, while during the "judicial procedure by the judge" [25]. Then, the measure of "seizure of objects and devices containing computer data" [25], as well as the measure of "copying and storing data that may serve as evidence" [25].

In cases where investigators cannot succeed through standard methods to obtain useful evidence regarding the identification of the perpetrator or clarification of the criminal offense, then the provisions of this law allow them to use "interception or recording of communication carried out by computer system equipment as investigative measures" [25].

Given that cybercrimes (including those committed in and from Kosovo) are often of an international nature (the largest number of servers that contain data on cybercrime perpetrators are still in the United States) [28], the law provides considerable space for Kosovo's international cooperation in this area. Kosovo's international cooperation in combating cybercrime under this law can be of various forms and consists of ranging from "international assistance, exchange of information to specialized training and other activities" [25].

Kosovo's government is prepared for secure international cooperation and has established a permanent contact point, which has numerous competences in this regard, including "rapid data storage and confiscation of equipment containing computer data" [25].

4.2 Law on Electronic Communications, 2012

This law regulates electronic communication in Kosovo [29]. Electronic communication is the activity of transferring ideas, knowledge, information, data or messages through digital means, including but not limited to communications via "fixed line, mobile phone, facsimile, Internet, cable, or satellite" [30].

Under this law, the development of electronic communications in Kosovo is defined by technological neutrality and the EU regulatory framework [29]. The law "promotes competition and guarantees proper and appropriate services" [29] for all operators who offer electronic communication services across all of Kosovo's territory. It is known that the European Convention on Human Rights guarantees and protects the right to respect for private and family life, as well as its correspondence [31]. Whereas the European Court of Human Rights, when interpreting the word "correspondence" has taken into account technological advances in the field of communication, therefore for the purposes of Article 8, the word "correspondence," it considers electronic communication in addition to old forms of communication [32]. Despite Kosovo is not a member of the Council of Europe, as a state, it has shown its readiness to respect the European Convention, determining with the provisions of this law that it "ensures an equal level of protection of the right to privacy and personal data of persons" [29].

The Kosovar legislator has taken into account the specifics of this contemporary form of communication, therefore, with the provisions of this law, it has defined some of the main principles for the regulation of this social activity. At the same time, competent bodies in this field have been arranged, with a focus on electronic communications that are developed for the purpose of national defense, national security, maintaining the state border, railway traffic safety, civil aviation, and the energy system.

Due to the significance of such communication for Kosovo's national security, this law stipulates that "the work of these institutions will be coordinated by the competent state institution" [29].

Public communications networks that consist of servers, firewalls, computers, routers, switches, printers, and more, often for the purpose of stealing, modifying, or removing access to valuable data, whether it be temporarily or permanently, are targeted by cybercrimes. As a result, with the provisions of Article 26, the law provides legal protection to public communications networks from all forms of cybercrimes [29].

In addition to the obligations for the state, the law also foresees obligations for entrepreneurs providing public communications networks, from whom it is required to undertake appropriate technical and organizational measures for the security of their networks and services. All these measures are designed to prevent and minimize attacks on electronic communication in Kosovo.

4.3 Law on Cyber Security, 2023

The need for Kosovo to have a legal framework for effective protection from cyberattacks was highlighted in the European Commission Report 2022 [33]. In the report during the assessment of the cyber security situation, it is noted that Kosovo has developed basic cyber security capabilities on the one hand, but on the other hand, it lacks a comprehensive legal framework, operational mechanisms, and technical and human capacities to operate effectively in the area of crimes and other illegal activities in cyberspace [34].

In order to harmonize its cybersecurity legislation, Kosovo has adopted this law, which partially transposes the EU Directive and the Council of Europe directive [35], then replaces the Council Framework Decision [36] as well as the European Parliament Directive [37] and the Council directive [38] on security measures for networks and information systems [39].

The law regulates important issues related to cybersecurity in Kosovo, such as defining the principles of cybersecurity and establishing institutions responsible for developing, implementing, and promoting cybersecurity policies [33].

The law stipulates the responsibilities for operators of essential services and the digital service provider's system, which impose permanent organizational requirements and physical and information technology security measures in order to prevent and combat cyber incidents as well [40].

In addition to these measures, the law requires operators to prepare a system risk assessment, then describe the measures for resolving a cyber incident, ensure the monitoring of the system to detect actions or software compromising its security, etc. [41].

Another obligation of the operator of essential services is to report a cyber incident to the Cyber Security Agency (CSA) "immediately, but not later than 24 hours after becoming aware of a cyber incident" [41].

The establishment of the Cyber Security Agency (CSA) and other relevant mechanisms for the implementation of cyber security measures in Kosovo is one of the most significant parts of this law. In addition to the CSA, this law also operationalizes the National Computer Emergency Response Team (CERT), then the State Council for Cyber Security (SCCS), the national sector-Computer Security Incident Response Team (CSIRTs), the State Training Center for Cyber Security, etc. [41].

Kosovo's legal framework is one of the most advanced in the region, furthermore, as per the EU Commission's Report on Kosovo in 2021, Kosovo's cybercrime law is generally in accordance with the EU *acquis* [42].

After reviewing the legislation on cyber security, it can be concluded that with the approval of the Law on Cyber Security (2023), Kosovo has somehow completed its legislation in the field of cyber security. More specifically, the Law on Prevention and Fight of Cybercrime (2010), has established the legal basis for preventing and combating cybercrime and sanctioning violations, adhering to human rights and protecting personal data [25]. In this law, cybercrime is defined as a criminal activity committed on a network that aims to misuse computer systems and computer data [43]. The Law on Electronic Communications (2012) provides legal guidelines for the use of electronic communication, as well as safeguarding personal data and the right to privacy in this area [44]. The Law on Cyber Security (2023) has a direct impact on strengthening cybersecurity in Kosovo, as the fulcrum of it was the Directives of the European Parliament and the Council of Europe of 2016 on security measures for network and information systems. This law governs the establishment of the National Cyber Security Authority and the operationalization of CERT within this structure. The provisions of this law enabled the strengthening of CERT's capacities, which were limited until this law was adopted.

In addition to its positive aspects, this legislation has its own weaknesses or shortcomings. Its weaknesses are considered as lack of harmonization between the provisions of these laws, despite the fact that all laws must be harmonized to have an adequate response to such attacks. The other shortcoming of this legislation is the spread of cybercriminal offenses and other legal violations through various laws.

As a good opportunity to avoid the non-harmonization of laws protecting cyber security and the spread of criminal offenses, there is the codification of legislation on cyber security.

Despite the above-stressed shortcomings and weaknesses, Kosovo has sufficient legislation to combat cybercrimes that is comparable to both the countries in the region and developed countries in Western Europe, including those of the EU.

5. Kosovo's main mechanisms for preventing and combating cybercrime

Kosovo, in order to protect itself and counter successfully the threats of cybercrime, besides raising funds and approving state strategies for cybersecurity (2023–2027), appropriate state mechanisms have also been established to combat cybercrimes, such as

1. The Cyber Security Agency (CSA);
2. State Council for Cyber Security (NCSC);
3. National Cyber Security Unit (KOS-CERT);
4. Kosovo Police Department for Cyber Security and Systems Administration;
5. State Cyber Security Training Center.

5.1 The Cyber Security Agency (CSA)

The Cyber Security Agency (CSA), established by Law on Cyber Security (2023), is the main institutional mechanism that is responsible for proposing and

implementing cybersecurity measures and ensuring cybersecurity throughout the country [1]. The CSA along with the State Council for Cyber Security (NCSC) acts as a regulatory body and creator of all state controls on cybercrimes. The agency was officially established by the government and serves as a central body for establishing, managing, auditing, and defending against malicious attempts [1]. This agency contributes to the increase of national capacities in the field of cyber security, so it has the duty to monitor, inspect, and coordinate the activities of the institutions responsible for cyber security, as well as to take measures in the event of not implementing the obligations stipulated by law for operators of essential services and digital service providers.

The CSA is also responsible for responding to threats and incidents in the cyberspace of the Republic of Kosovo and recording them in the cyber threats register, furthermore to create an electronic platform for information exchange, which platform can be used by all operators of essential services and digital service providers in Kosovo. The agency cooperates with the authorities of foreign countries and international organizations regarding aspects under the responsibility of the CSA and serves as the single point of contact. The CSA coordinates its activities with security and defense institutions and cooperates with national sectorial cyber security incident response teams, designated information security officials, and international authorities [41]. The CSA has established a communication platform for citizens and businesses that is available 24/7 for reporting cyber incidents.

5.2 State Council for Cyber Security (NCSC)

The NCSC is an advisory independent body of the Government of Kosovo and the business community, which takes strategic measures to increase the level of cyber security in the Republic of Kosovo. The NCSC is responsible for enhancing coordination and cooperation between various public institutions that have competence in cyber security matters, as well as between the public and private sectors. The advisory body is composed of high-level representatives from government institutions, law enforcement agencies, public and private organizations, and the scientific community. It will also facilitate the decision-making process by analyzing, studying, and proposing initiatives at national and international levels [41]. The NCSC achieves its mission by providing strategic advice on cybersecurity to the Government of Kosovo and the business community (through the government), observing the latest technological trends and developments and, when needed, taking measures to reduce cyber security risks, to increase economic opportunities, and initiating and accelerating relevant initiatives that significantly contribute to increasing the level of cyber security in Kosovo; systematically monitoring and coordinating the implementation of the National Cyber Security Strategy, taking into account all current and future challenges in the field of cyber security, suggestion of precise measures to improve the implementation of the National Cyber Security Strategy and Action Plan, etc. [41]. The NCSC is headed by the Minister of Ministry of Internal Affairs or his delegate, who is *ex officio* the National Coordinator for Cyber Security.

Otherwise, the regular annual meetings of the NCSC are known to the Kosovo public, in which the members are informed and discuss the level of cyber security in Kosovo, then the implementation of the State Strategy for Cyber Security is evaluated during the period between the two NCSC meetings; also the measures and activities that have been taken and those that will be undertaken to increase cyber security in all public institutions are discussed. But when the need calls for it, and especially

when the institutions of Kosovo are attacked by cybercrimes, then the NCSC also holds extraordinary meetings, as was the case with the cyberattacks in March 2021, when discussing the type of cybercrime (DDoS), the consequences caused, and the measures taken, also notified the dependent institutions and the persons responsible for the steps they need to take [45].

5.3 National Cyber Security Unit (KOS-CERT)

The National CERT (Computer Emergency Response Team) is the team of the Republic of Kosovo that responds to computer emergencies at the national level [41]. Besides this team, the Kosovo legislation allows for the establishment of teams in specific sectors of critical infrastructure. These are the teams responsible for responding to computer security or cyber security incidents that affect an operator of essential services (CSIRTs of operator essential services- OES) and the teams responding to computer security or cybersecurity incidents affecting digital service providers (CSIRTs of digital signal processors- DSPs) that also operate in Kosovo.

The Regulatory Authority of Electronic and Postal Communications (ARKEP) is the national body responsible for the regulation of electronic communications activities, as outlined in the Law of Kosovo on Electronic Communications (2012). Article 10 mandates and obligates the authority to "perform the functions of the Computer Center for Emergency Response to manage risks in public electronic communications systems" [44]. The authority incorporated and functionalized the KOS-CERT in July 2016 as a technical and functional unit. The National KOS-CERT is authorized to handle all types of computer security incidents that occur or threaten to occur in the Kosovo community environment. KOS-CERT is dedicated to keeping the community informed about potential risks and will inform them before they occur if possible.

Otherwise, KOS-CERT is one of the first units of this type from the region that was accredited in July 2017 by the "Trusted Introducer/TF-CSIRT," which was created by the European community of CERTs (Computer Emergency Response Teams) in 2000 to address common needs and establish a service infrastructure that provides vital support to all cybersecurity teams.

The functionalization of KOS-CERT in July 2016 has had a direct impact on the establishment of the CSIRTs. Thus, in Kosovo, during the period 2016–2020, more than 50 CSIRTs have been functionalized and have started operating [43].

Despite KOS-CERT's creation of an online platform that allows Kosovo citizens to report cyber incidents against both private and public legal entities and citizens, in the absence of awareness of its existence, victims of cybercrime do not use it. However, such cases are reported to the Kosovo Police, which further transmits them to its Investigations Department and Cybercrime Investigation Section [43].

5.4 Kosovo Police Department for Cyber Security and Systems Administration

Given the high risk of cybercrimes, the Ministry of Internal Affairs of Kosovo has established the Cyber Security Department. One of its main duties is to prepare, supervise, and implement cybersecurity policies at the national level. In addition to tasks of a strategic nature, the department is also responsible for the practical level of combating cybercrimes because it coordinates cyber security activities related to various cyber incidents. Regardless, they are committed to public or private institutions. Within the Kosovo Police, the investigation of cybercrime is handled by the

cybercrime investigation sector, which is part of and operates within the Directorate for the Investigation of Organized Crime.

The cybercrime investigation sector deals with citizens' denunciations related to cybercrimes, taking investigative actions, such as crime scene investigation, interrogation of suspects, victim interviews, and various computer expertise in order to detect and fix traces and evidence of cybercrimes.

5.5 State Cyber Security Training Center

The State Cyber Security Training Center operates within the Ministry of Defense of Kosovo in order to provide training for all institutions of the Republic of Kosovo in the field of cyber security. The Center has its own organizational structures, which, in cooperation with CSA, determines the procedure and format of specialized programs for training and certification of personnel engaged in the field of cyber security in accordance with their competencies [41].

To fulfill its obligations, The Center collaborates with numerous international projects and mechanisms. Particularly, during the preparation and finalization of the training curriculum for its beneficiaries in September 2023, the activities of this Center were supported by the program of the British Embassy in Prishtina and implemented by the Geneva Centre for Security Sector Governance (DCAF).

Given that the individual actions of the above-mentioned mechanisms may be accompanied by omissions and inefficiencies in the fight against cybercrime, as per the Law on Cyber Security (2023), it has been determined that state mechanisms for preventing cyberattacks and cyber protection in the Republic of Kosovo must coordinate and cooperate between them during full filling of their duties and responsibilities.

Kosovo has completed its state mechanisms for combating cybercrime with the establishment of the State Agency for Cyber Security. The State Agency for Cyber Security and the NCSC acts as a regulatory body and creator of all state controls. The updated legislation of Kosovo with which these mechanisms are established is being reviewed by the NIS European Directives, as an attempt to remove redundancies and make it as relevant as possible [46]. These mechanisms, which are relatively new and lack experience, are experiencing difficulties of different natures, which are affecting their low-efficiency rate. Among the difficulties of these mechanisms are considered:

- Institutions are experiencing a significant shortage of cybersecurity experts in the country.
- Victims of cybercrime are not using the Kos-CERT online platform for cyber incident reporting because they are unaware of its existence.
- The lack of clarification of clear mandates and competencies with legal provisions of these mechanisms.
- Lack of transparency and accountability culture among essential state service operators is expressed through non-publication of reports on cybersecurity incidents.
- Insufficient cooperation of these mechanisms (e.g., KOS-CERT) with academic institutions is due to limited professional capacities, etc.

Therefore, Kosovo's state institutions have a priority task to take various measures to improve the functioning of cyber security protection mechanisms.

6. Conclusions

The rise in computer users and Internet services has led to an increase in cybercrimes worldwide, including in Kosovo.

During the last few years, Kosovo has been attacked with both ordinary forms of cybercrime and forms that have threatened the national security of this country. Cybercrime has hindered and threatened the operation of some of the highest state institutions, beginning with the Presidency, the Prime Minister's Office, the Ministry of Foreign Affairs of Kosovo (MFAK), the Ministry of Internal Affairs of Kosovo (MIAK), the Prosecutor's Office of Kosovo, etc.

Kosovo's national security has also been endangered by propaganda, disinformation, and fake news spread by opponents of Kosovo's independence, such as Serbia, Bosnia and Herzegovina, Russia, and other countries in this political bloc. The purpose of this cyber propaganda is to manipulate the citizens of Kosovo and escalate the situation on the ground, causing a conflict between the majority Albanians and the minority Serbs in Kosovo.

Cybercrime in Kosovo has included information about threats to Kosovo institutions, such as bomb explosions.

The most frequent types of cybercrime threatening Kosovo's national security include Distributed Denial of Service (DDoS) and "Phishing" as a form of "social engineering" that aims to steal credentials.

The digitization of state institutions in Kosovo, which process data for almost 1.7 million citizens, poses a risk and possibility of increasing cyber threats and cybercrimes in Kosovo.

The Republic of Kosovo faces numerous challenges in combating cybercrime, starting from the lack of human resources in the state institutions to build cyber security capacities, then the courts are not professionally prepared to properly handle cybercrime cases, the decentralization of computer systems in Kosovo's institutions, lack of harmonization between different laws, strategies and other acts in this field. Another challenge for Kosovo is building capacities to combat existing cybercrimes (more than 50 types) and adapt to new types that may appear and endanger its security.

Kosovo's legislation on cyber security, in addition to being harmonized with *aquis communiter*, provides legal security for Kosovo citizens because, among others, it protects the confidentiality, integrity, and availability of computer system data; contains a significant number of criminal offenses from the sphere of cybercrimes and determines the criminal sanctions for their perpetrators; considers and regulates the issue of respect for human rights.

Kosovo's legislation on cyber security also deals with the international cooperation of Kosovo's institutions with mechanisms similar to those in other countries in preventing and fighting cybercrime as well as regulating other issues in the field of cybersecurity.

Kosovo has set up the necessary mechanisms and institutions to combat cybercrime, including The Cyber Security Agency, the State Council for Cyber Security, the National Cyber Security Unit, the Kosovo Police Department for Cyber Security and Systems Administration, and the State Cyber Security Training Centre.

In order to enhance the effectiveness of these mechanisms and successfully overcome the challenges related to cybersecurity, state institutions, and Kosovo society in general should take certain measures related to:

- Providing cybersecurity training programs for both government employees and private sector workers.
- Making regular cybersecurity training mandatory for all essential state services.
- Raising awareness among staff members of these mechanisms and citizens of Kosovo about cybersecurity threats.
- Granting assistance to academic institutions and private companies in the development of new tools and technologies to tackle emerging cyber threats.
- Collaboration between government agencies, private companies, and academic institutions can be encouraged by a state to exchange information and expertise on cybersecurity threats, best practices, etc.

Author details

Haki Demolli
Law Faculty, Department of Criminal Law, University of Prishtina, Kosova

*Address all correspondence to: haki.demolli@uni-pr.edu

References

[1] Hughes BB, Bohl D, Irfan M, Margolese-Malin E, Solórzano J. Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance. Zurich, Switzerland: Zurich Pardee Center; 2015. p. 4. Available from: https://korbel.du.edu/pardee/resources/cyber-benefits-and-risks-quantitatively-understanding-and-forecasting-balance/

[2] Eurostat. Enlargement Countries - Information and Communication Technology Statistics. 2023. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Enlargement_countries

[3] Kroçi V. Kosovo's Take on Cybersecurity. Prishtina, Kosovo: Securitybrief; 2023. Available from: https://qkss.org/images/uploads/files/Security_Brief_-Vesa_Kroci.pdf/

[4] Klopfer F, Rizmal I, Sekuloski M, Hatzl T, Mladenovic D. Introduction to Cybersecurity Governance—A Tool for Members of Parliament. Genevea, Switzerland: Geneva Centre for Security Sector Governance (DCAF). p. 7

[5] Klan Kosova. Institucionet e Kosovës cak i sulmeve kibernetike nga Beogradi (Belgrade is Targeting Kosovo Institutions with Cyber Attacks). Prishtina, Kosovo: Klan Kosova; 2018. Available from: https://klankosova.tv/institucionet-e-kosoves-cak-i-sulmeve-kibernetike-nga-beogradi/

[6] Rexha A. Vulnerability Index of Disinformation in Kosovo. Prishtina, Kosovo: Democracy Plus; 2022. p. 20

[7] NDI-Kosovo. Information Integrity Challenges: A Growing Threat to Kosovo's Democracy. Prishtina, Kosovo; 2021. p. 8

[8] Baftiu D. Siguria kibernetike në Kosovë, fushë e re me shumë sfida (Cyber Security in Kosovo is a New Field with Many Challenges). Prague: Radio Free Europe; 2023. Available from: https://www.evropaelire.org/a/siguria-kibernetike-kosove/32597883.html/

[9] Telegrafi. Cybersecurity in Kosovo, How Much are We at Risk? Prishtina, Kosovo: Telegrafi; 2023. Available from: https://telegraficom.translate.goog/siguria-kibernetike-ne-kosove-sa-jemi-te-rrezikuar/

[10] Jaha S. Alarmante: Ministria e Punëve të Brendshme cak i sulmeve kibernetike (Alarming: The Ministry of Internal Affairs is the target of cyberattacks). Prishtina, Kosovo: Infokus; 2022. Available from: https://gazetainfokus.com/alarmante-ministria-e-puneve-te-brendshme-cak-i-sulmeve-/

[11] Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Cardiff, United Kingdom: Frontiers in Computer Science. Cardiff School of Technologies; 2021. p. 3. Available from: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full/

[12] Carroll F, Adejobi JA, Montasari R. How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. SN Computer Science. 2022;**3**(2):170. DOI: 10.1007/s42979-022-01069-1. Epub 2022 Feb 23

[13] Hoyos Ll MS, Isaza E GA, Vélez JI, Castillo OL. Distributed denial of service (DDoS) attacks detection using machine learning prototype.

In: Omatu S et al., editors. Distributed Computing and Artificial Intelligence, 13th International Conference. Advances in Intelligent Systems and Computing. Vol. 474. Cham: Springer; 2016. p. 1. DOI: 10.1007/978-3-319

[14] Llozani L. MPB e konfirmon sulmin kibernetik ndaj institucioneve (The Ministry of Internal Affairs confirms the cyberattack on the institutions). Prishtina, Kosovo: Dukagjini; 2023. Available from: https://www.dukagjini.com/mpb-e-konfirmon-sulmin-kibernetik-ndaj-institucioneve/

[15] In accordance with Article 327 of the CCK, if someone commits a common form of criminal offense, they can be punished with a fine and imprisonment for up to three (3) years. If the criminal offense results in a financial benefit for the perpetrator or property damage for the victim that exceeds 10,000 euros, then the perpetrator can be sentenced to imprisonment from six months to five years, in addition to a fine

[16] Article 199 of the CCK allows for a fine and imprisonment for up to one (1) year to be imposed on the perpetrator of this criminal offense in its ordinary form

[17] The Kosovo Judicial Council (KJC) is a constitutional institution that, among other things, decides on the organization, management, administration, and oversight of the proper functioning of the courts in Kosovo, according to the Law

[18] Kosovo Statistics Agency. Women and Men in Kosovo 2014-2015. Prishtina, Kosovo; 2016. p. 53

[19] According to Kafexholli H. Sulmet kibernetike rriten në Kosovë, cak kryesisht mediet (Cyberattacks are Increasing in Kosovo, Mainly Targeting the Media). Prishtina, Kosovo: Nacionale; 2023. Available from: https://nacionale.com/drejtesi/sulmet-kibernetike-rriten-ne-kosove-cak-kryesisht-mediet-ekspertet-alarmojne-per-gjendjen//, local expert Butrint Komoni, has stated that the Government of Kosovo had a plan to establish a state academy for the training of young people for protection from cyberattacks, then they would be sent to work in the Ministry of Defense of Kosovo, for a salary monthly of 600 euros. On this occasion, he makes the question "who will work in state institutions for a salary of 600 Euros, when I am ready to pay them at least 1200 Euros in my private business. To conclude that the USA also has problems of this nature"

[20] Elwood K. Ransomware Poses Threat to Vulnerable Local Governments. USA: The Washington Post; 2021. Available from: https://www.washingtonpost.com/local/local-governmentransomware-dc

[21] Kafexholli H. Sulmet kibernetike rriten në Kosovë, cak kryesisht mediet (Cyberattacks are Increasing in Kosovo, Mainly Targeting the Media). Prishtina, Kosovo: Nacionale; 2023. Available from: https://nacionale.com/drejtesi/sulmet-kibernetike-rriten-ne-kosove-cak-kryesisht-mediet-ekspertet-alarmojne-per-gjendjen/

[22] Shruti M. Types of Cyber Attacks You Should Be Aware of in 2024. USA: Simplilearn; 2023. Available from: https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks/: In the article, he outlines the existence of 54 cyber crimes, with a focus on 10 main ones: Malware; Phishing; Password Attack; Man-in-the-Middle Attack; Structured Query Language (SQL) injection attack; Denial-of-Service Attack; Insider Threat; Cryptojacking; Zero-Day Exploit; Watering Hole Attack etc

[23] Butrint Komoni, the cyber science expert, gave an assessment regarding

the cyber skills of the staff of the Kosovo justice system in his statement in the journalistic article. Kafexholli H. Cyber Attacks are Increasing in Kosovo, Mainly Targeting the Media - Experts Warn about the Situation. Nacionale; 2023. Available from: https://nacionale.com/drejtesi/sulmet-kibernetike-rriten-ne-kosove-cak-kryesisht-mediet-ekspertet-alarmojne-per-gjendjen/

[24] NordLayer. The Evolution of Cyber Threats: Looking Back Over the Past 10 Years. 2023. Available from: https://nordlayer.com/blog/evolution-of-cyber-threats-over-10-years/

[25] Kosovo's Law on Prevention and Fight of the Cyber Crime (2010), Article 1; Article 3; Article 9 paragraph (1); Article 9, paragraph (3); Article 17; Article 3 and Article 20, paragraph (2)

[26] Bagovic K. Sankcioniranje cyber nasilja prema novom Kaznenom zakonu. IUS-INFO - Sankcioniranje cyber nasilja prema novom Kaznenom zakonu (iusinfo.hr); 2012

[27] Babić V. Kompjuterski kriminal: Metodologija kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminala, Sarajevo, BiH. RABIC Sarajevo; 2009

[28] Potrka N. Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru (doktorska disertacija). Zadar, Croatia; 2018. p. 58

[29] The law was approved by the Assembly of Kosovo, dated 04.10.2012, with no. 04/L-109

[30] Gürkaynak G, Yilmaz I. Nazli Pinar Taskiran: 'Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age'. Computer Law & Security Review. 2014;**30**(2):179-189

[31] The European Convention on Human Rights; Council of Europe 2012, Article 8

[32] Roagna I. Protecting the Right to Respect for Private and Family Life Under the European Convention on Human Rights. Brussels, Belgium: Council of Europe; 2012. p. 28

[33] This law was approved by the Assembly of Kosovo on 27.02.2023, with number 08/L-173

[34] Buzhala J. Gjoba e paralajmërime për burg për "hakerët" nga Kosova (Kosovo's "Hackers" are Facing Fines and Prison Warnings). Prishtina, Kosovo: Kallxo.com; 2023. Available from: https://kallxo.com/gjate/gjoba-e-paralajmerime-per-burg

[35] Directive (EU) 2013/40 of the European Parliament and of the Council of 12 August 2013

[36] Council Framework Decision 2005/222/JHA

[37] Directive (EU) 2016/1148 of the European Parliament

[38] Directive of the Council of 6 July 2016 on security measures for network and information systems

[39] Article 109 of The Kosovo's Law on Electronic Communication, says : 'There shall be repealed Law no. 2002/7 on Telecommunications, dated 12.05.2003 and Law No.03/L-085 on amending Law on Telecommunication, dated 13.06.2008'

[40] Elshani (KCSS) D. Are Non-Governmental Organizations Prepared to deal With Cyberthreats? Prishtina; 2023. p. 7

[41] The Kosovo's Law on Cyber Security, 2023, Article 1, paragraph (2); Article 6,

paragraph (1); Article 7 and 8; Article 24; article 16; Article 5; article 3 paragraph (1.22); Article 2 paragraph (2)

[42] European Commission. Commission Staff Working Document - Kosovo* 2023 Report. Accompanying the document Communication from the Commission to the European Parliament, the Council. Brussels: The European Economic and Social Committee and the Committee of the Regions 2023; Communication on EU Enlargement Policy; 2023. p. 50

[43] Peci L, Ukshini (Kipred) V. Good Governance in Cyber Security in Kosovo: Strengthening the Foundations and New Institutions. Prishtina; 2022. p. 6

[44] The Law on Electronic Communications of Kosovo (2012), Article 1 and 2; Article 85 paragraph (1) and Article 10

[45] Sinjali. Pas raportimeve për sulme, Këshilli Shtetëror për Siguri Kibernetike mbajti një takim (The State Cyber Security Council held a Meeting after Receiving Reports of Attacks). Prishtina, Kosovo: Sinjali; 2021. Available from: https://sinjali.com/pas-raportimeve-per-sulme-keshilli-shteteror-per-siguri-kibernetike-mbajti-nje-takim/

[46] Balkans Policy Research Group. Kosovo in the Face of Cybersecurity Threats: Critical Actions to Consolidate Resilience. 2023. p. 9. Available from: https://balkansgroup.org/wp-content/uploads/2023/09/Cyber-Security.pdf

Section 3

Future Innovation in National Security

Chapter 6

Cyber Orbits: The Digital Revolution of Space Security

Ulpia-Elena Botezatu and Adrian-Victor Vevera

Abstract

This chapter navigates the intricate landscape of space security in the digital age, exploring the interplay between cybersecurity and the protection of outer space assets. In light of our ever-growing dependence on digital technology and the global exchange of information, traditional concepts of national and global security are experiencing a fundamental evolution. The chapter's exploration spans from dissecting the concept of national security in the digital age to investigating how global digital dialogs profoundly shape space security. It sheds light on the critical convergence of cyber threats and space security, underscoring the vulnerabilities found in outer space infrastructure. Insightful scrutiny of information warfare within the context of space, ethical considerations surrounding digital surveillance practices, and the collaborative engagement of various stakeholders are thoroughly examined. Ultimately, the chapter advocates for a post-structuralist approach to comprehensively grasp and effectively confront the multifaceted challenges arising in this swiftly evolving domain.

Keywords: cybersecurity, space security, information warfare, space surveillance and tracking, global security

1. Introduction

In the twenty-first century, the integration of digital technology with space operations generated a transformative shift in the operational paradigms of outer space activities [1]. This confluence has both expanded the frontiers of space exploration and provoked a complex array of cybersecurity challenges that imperil the integrity and functionality of space assets [2]. As nations and private entities increasingly rely on satellite systems for communication, navigation, timing, remote sensing, and other critical services, the cybersecurity of space-based systems has risen to the forefront of global security infrastructure [3].

The significance of cybersecurity within the domain of space security cannot be overstated. Cyber threats targeting space assets encompass a broad spectrum of activities, ranging from incursions into satellite communication channels to the disruption of ground control operations and interference with data transmission processes. These threats have the potential to incapacitate national defense systems, disrupt global telecommunications, and compromise critical infrastructure, thereby amplifying the cybersecurity of space systems into a matter of national and international concern [4, 5].

From the outset of this exploration into space security within the digital age, it is essential to engage with the foundational perspectives of structuralism and post-structuralism, providing a nuanced framework for this analysis. Structuralism, a theoretical paradigm that emphasizes the identification and understanding of the underlying structures governing human society and culture, offers a lens through which we can examine the organized frameworks and systems that define space security operations. Theories from Claude Lévi-Strauss and Ferdinand de Saussure provide a methodological foundation for dissecting the stable, invisible structures that underpin the global cybersecurity landscape [6, 7]. Conversely, post-structuralism, emerging as a critique of structuralism's rigidity, challenges these established norms and assumptions. Inspired by the works of Michel Foucault and Jacques Derrida, post-structuralist theory invites us to boldly question the power dynamics and discursive formations that shape our understanding of cybersecurity in space, advocating for a more fluid and nuanced interpretation of these complex systems [8, 9]. By weaving these theoretical lenses throughout our discussion, we hope to achieve a dynamic and comprehensive examination of the multifaceted challenges space security faces in the digital era. The objective of this chapter is to shed light on the intricate relationship between cybersecurity and space security in the digital age. Initially, it expands upon the metamorphosis of national security paradigms in response to digital advancements, clarifying how the digital sphere has reshaped traditional perceptions of security. Subsequently, the discussion will transition to the global digital discourse and its ramifications for space security, examining how international endeavors to establish cyber norms and regulations influence space operations. The confluence of cybersecurity threats with space security concerns will be probed in detail, outlining the vulnerabilities endemic to space infrastructure and their ramifications for global security. Moreover, this narrative will encompass the realm of information warfare, illustrating this contemporary form of conflict and its challenges to established norms in space security. Additionally, the chapter will scrutinize the impact of digital surveillance technologies, ethical considerations, and the pivotal roles played by diverse stakeholders in navigating the cybersecurity landscape of space operations. To fully address these challenges, an interdisciplinary approach that integrates both structuralist and post-structuralist theories from the beginning, rather than relegating them to the concluding analysis, enriches our understanding and response to the evolving threats within space security. The concluding section will advocate for a post-structuralist approach to comprehend and address the multifaceted challenges posed by the digital revolution in space security. Through a critical exploration of information warfare and its manifestations in space, we will delve into specific incidents or examples of information warfare tactics in action, portraying the complexities and strategic implications associated with this emerging form of conflict.

2. Deconstructing national security in the digital age

Digital technology operated profound transformations in the paradigms of national security. Traditionally rooted in physical borders and military ability, and transformed by the Copenhagen School of International Relations [10], national security now faces a redefinition within the context of cyberspace and information technology [11]. This evolution reflects the growing recognition that cybersecurity threats pose a significant risk to national infrastructure, undermining a nation's economic, social, and political stability without a single physical incursion. Concrete

examples such as the 2015 cyberattack on Ukraine's power grid, which left hundreds of thousands without electricity, underscore the vulnerability of critical infrastructure to cyber threats, thereby manifesting the potential for such vulnerabilities to profoundly affect the daily lives of citizens and the functioning of societies [12]. Moreover, the global nature of cyberspace further complicates national security in the digital age. Cyber threats, illustrated by incidents like the 2017 WannaCry ransomware attack impacting over 150 countries [13], transcend national borders, rendering response efforts intricate, underscoring the imperative for international cooperation in cybersecurity endeavors and the holistic reassessment of traditional security frameworks.

The tangible impact of cybersecurity incidents targeting national infrastructure has served as a clear indication of these emerging threats. For instance, the 2015 cyberattack on Ukraine's power grid, which left hundreds of thousands without electricity, underscored the vulnerability of critical infrastructure to cyber threats and the potential for such vulnerabilities to be exploited, affecting the daily lives of citizens and the functioning of societies [12, 14].

Cyber threats often transcend national borders, rendering attribution and response efforts intricate. The 2017 WannaCry ransomware attack, which impacted more than 150 countries, brought to light the transnational dimension of cyber threats and underscored the imperative for international cooperation in cybersecurity endeavors [13].

At the forefront of national security in the digital age are pivotal national cybersecurity strategy documents outlining comprehensive approaches to safeguard critical infrastructure, disrupt cyber criminals, and engage with international partners to fortify global cybersecurity. For example, the United States' National Cyber Strategy delineates a comprehensive approach to strengthen critical infrastructure, combat cyber criminals, and foster international collaboration to bolster global cybersecurity [15]. Similarly, the European Union's Cybersecurity Strategy endeavors to enhance cyber resilience, mitigate cybercrime, and establish a framework for international cooperation in cyberspace [16].

Looking at national security through the epistemological lenses offered by structuralism and post-structuralism, helps us maintain a sharp focus on national security and defense while mapping a wide array of threats as well as perceptions of threats, risks, and vulnerabilities. This early integration of structuralist and post-structuralist theories into our discussion not only deepens our analysis but also primes the reader for a more nuanced understanding of the challenges and strategies in cybersecurity and space security as they evolve throughout Section 3. The global discourse on cyber norms and regulations has assumed pivotal significance in shaping the operational and security paradigms of space activities. This section seeks to examine the impact of such international dialogs and agreements on the governance and security of outer space activities [17], with a dedicated focus on the pivotal role played by key international bodies.

In exploring the convergence of cybersecurity threats and space security, this chapter navigates through the structured paradigms of international cooperation and cybersecurity efforts within the realm of outer space activities. Drawing upon Claude Lévi-Strauss's structuralist framework, we initially decipher the underlying infrastructures that govern space security policies and practices [6]. This foundational analysis is pivotal for understanding how global security measures are architected and implemented. However, recognizing the limitations of structuralist approaches in addressing the fluid and evolving nature of cybersecurity threats, we then invoke

Michel Foucault's post-structuralist critique of power relations and knowledge systems [8]. Foucault's insights allow us to question the efficacy and inclusiveness of existing security protocols, suggesting that the power dynamics embedded within the discourse of space security may obscure or neglect emerging threats and challenges.

Furthermore, Jacques Derrida's concept of deconstruction [9] is employed to unravel the assumptions and binary oppositions—such as secure/insecure, threat/non-threat—that underpin traditional cybersecurity frameworks. Through this deconstructive lens, we identify the potential for reinterpretation and reconfiguration of space security measures, advocating for a more adaptive and nuanced approach that is responsive to the complex interplay between technological advancements and cybersecurity challenges. This integrated structuralist and post-structuralist analysis illuminates the complexities of safeguarding space infrastructure, highlighting the need for ongoing critical evaluation and innovation in security strategies to ensure the resilient and sustainable use of outer space.

The concerted efforts of international organizations, such as the United Nations Office for Outer Space Affairs (UN OOSA) and the International Telecommunication Union (ITU), have been instrumental in fostering international cooperation for the peaceful use and exploration of outer space. Through their comprehensive work, including the Guidelines for the Long-term Sustainability of Outer Space Activities [18], UN OOSA has laid the groundwork for a collaborative approach to confronting the cybersecurity challenges confronting space assets and operations. The ITU's emphasis on ensuring secure and reliable communication links, as outlined in their latest reports and regulations, directly impacts satellite communications and global connectivity [19, 20]. Similarly, the ITU's emphasis on ensuring secure and reliable communication links assumes particular relevance in the context of satellite communications, where vulnerabilities may have far-reaching implications for global connectivity and security. Additionally, the United Nations has initiated several projects aimed at strengthening cybersecurity in space, including the recent resolution discussed by the General Assembly to promote international collaboration in this area, as well as the work of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security [21].

Reflecting upon the series of UN resolutions designed to enhance cybersecurity within the space domain [21, 22], the applicability of Foucault's theories on power relations and knowledge construction becomes evident in the formation and interpretation of international norms [8]. These resolutions not only underscore the imperative for member states to enact protective measures against cyber threats but also illuminate the power dynamics involved in the creation and adoption of global security standards. Furthermore, viewing these normative frameworks through the lens of Derrida's deconstruction theory [9], prompts critical inquiry into whose interests are served by these norms and how they might be reinterpreted to more accurately reflect the emerging realities of space security. Thus, the discussion surrounding UN resolutions is enriched by acknowledging that, while they serve as responses to cyber threats, they are also manifestations of complex power structures, warranting detailed examination.

The proactive engagement of international bodies, such as the ITU and UN OOSA, through their regulations, guidelines, and collaborative projects, provides a solid foundation for this evolution. However, a deeper understanding and application of theories such as those proposed by Foucault and Derrida enable a critical examination of these efforts, urging continuous adaptation and innovation. Thinking through the lenses of post-structuralist theory not only enriches our understanding of the

cybersecurity landscape in space operations but also challenges us to rethink and redefine the parameters of space security in the digital age. By critically engaging with the constructs of power and knowledge that shape space security discourse, this chapter advocates for a more inclusive and dynamic framework that is capable of addressing the multifaceted challenges posed by cyber threats to space assets and operations. This reevaluation is essential as we advance toward a more interconnected and digitally reliant space environment, where traditional security paradigms must evolve to address the nuanced and ever-changing landscape of cyber threats.

3. Convergence of cyber and space security threats

The convergence of cyber and space security threats represents a critical frontier in the protection and maintenance of global communication, navigation, and surveillance systems. The integrity of space infrastructure, encompassing both outer space assets, that is, satellites and ground stations, stands as a critical cornerstone for national security, scientific inquiry, and commercial endeavors. However, the digitization of space operations has exposed these assets to cyber threats, ranging from signal manipulation and spoofing to unauthorized access and control of satellite systems.

These vulnerabilities, often stemming from outdated security protocols and the utilization of commercial off-the-shelf technologies, pose significant risks as adversaries may exploit them to disrupt communication channels or manipulate data [23, 24]. Notable instances, such as the 2007 cyber intrusion compromising the control systems of a commercial satellite and the 2014 cyber intrusions targeting satellite ground stations, underscore these risks vividly. These incidents not only highlight the tangible risks posed by cybersecurity threats to space security but also emphasize the imperative for robust security measures and international cooperation to shield space assets from malicious cyber activities.

The vulnerabilities in space infrastructure seen from a cybersecurity standpoint stem from various factors, including the reliance on legacy systems employing outdated security protocols, the utilization of commercial off-the-shelf technologies that may lack robust security measures, and the intricate nature of international collaborations that complicate the establishment of unified security standards [2]. These vulnerabilities indicate significant risks, as adversaries may exploit them to disrupt communication channels, manipulate data, or even seize control of critical satellite functions. Some space systems still use hardcoded credentials, which can be exploited by attackers. Vulnerabilities in onboard software can lead to unauthorized control or data manipulation, in addition to those vulnerabilities that could be introduced by various vendors of components mounted on satellites and other space assets.

A striking instance that illustrates the intersection of cybersecurity threats and space security unfolded in 2007 and 2014 when several countries reported unauthorized access and interference with their satellite operations [25]. Other examples are demonstrated by insurgents intercepting and decoding surveillance video in Iraq in 2009 and hackers seizing control of NASA's Terra earth observing system (EOS) for extended periods in 2008 [26]. These cyber intrusions, attributed to state-sponsored actors, involved the exploitation of vulnerabilities in satellite communication systems and ground control stations, resulting in transient disruptions and the potential for graver consequences had the attacks escalated [23, 27].

These examples serve as a clarion call for the implementation of comprehensive security protocols and the fostering of international collaboration. By understanding these vulnerabilities and responding with concerted efforts, the international community can better protect the vital infrastructure that underpins both national and global security in the space domain.

4. Information warfare in space

The advent of digital technology has expanded the domain of space operations and introduced sophisticated forms of conflict, notably information warfare, into the extraterrestrial domain. Information warfare, a concept historically confined to cyberspace and electronic communication channels on Earth, has transcended atmospheric boundaries, emerging in space through advanced tactics such as signal jamming and global navigation satellite system (GNSS) spoofing. These tactics epitomize a significant shift in the nature of military operations [28], extending the theater of war into space, where control over information and communication lines becomes a pivotal aspect of strategic dominance [29, 30].

The extension of information warfare into space necessitates a reevaluation of existing security protocols and the development of innovative countermeasures to protect space infrastructure. By integrating cyber resilience frameworks, along with the adoption of advanced encryption technologies and intrusion detection systems, the international space community asserts its commitment to preserving the integrity of space operations amidst the burgeoning threats of information warfare [2, 24].

Moreover, international cooperation and the establishment of norms and regulations governing the use of space for military purposes become essential in mitigating the risks associated with information warfare in space [28]. Initiatives led by organizations such as north atlantic treaty organization (NATO), in conjunction with dialogs in international forums, play a pivotal role in shaping a collective response to these emerging challenges, underscoring the importance of collaborative efforts in securing the space domain in the era of digital conflict [1, 29]. The criticality of such cooperation is highlighted by the ongoing efforts to develop a comprehensive legal and ethical framework for space operations, ensuring a balanced approach to space security that encompasses both military and civilian interests. Moreover, ongoing research focuses on the development of post-quantum algorithms, aimed at bolstering resistance against potential quantum attacks. Given the long lifecycles of space systems, the implementation of quantum-safe cryptography is crucial to ensuring enduring security and resilience.

5. Digital surveillance, ethics, and space

The rapid technological advancements have significantly expanded surveillance capabilities, particularly through space-based technologies such as satellites equipped with high-resolution imaging and signal interception capabilities. While serving as a powerful tool for ensuring national security, the omnipresent surveillance apparatus simultaneously poses significant risks to individual privacy and civil liberties, leading to an ethical quandary surrounding the potential misuse of these technologies. These ethical dilemmas were underscored by the global surveillance disclosures of the early twenty-first century, prompting calls for a reassessment of surveillance practices and oversight mechanisms.

Reports from organizations such as Privacy International [31] and the Electronic Frontier Foundation [32] provide valuable insights into the potential overreach of surveillance practices, advocating for stringent safeguards to protect individual rights in the digital age. The pressing need for ethical considerations within digital surveillance through space technologies must be met with robust regulatory frameworks and oversight mechanisms to ensure the responsible and ethical use of space-based surveillance technologies. The delicate balance between leveraging these technologies for security and prioritizing individual rights underscores the imperative for ethical vigilance, global cooperation, and continuous assessment of the ethical implications of space-based surveillance.

The ethical dilemmas pertinent to digital surveillance in space were underscored by the global surveillance disclosures of the early twenty-first century. These revelations brought to light the extent to which governments could intercept personal communications and track individuals on a global scale, prompting a worldwide debate on privacy rights and state surveillance. The profound impact of these disclosures on international relations prompted calls for the reassessment of surveillance practices and oversight mechanisms, highlighting the delicate balance needed between leveraging space technologies for security and upholding ethical standards and respect for privacy.

Given the rapid pace of technological advancement and the international nature of space, a critical need arises for a global dialog on the establishment of norms and regulations that govern the use of space for surveillance purposes. Studies and policy analyses offer a foundational framework for understanding the complexity of space surveillance ethics [33]. These studies elucidate the challenges and propose pathways toward equitable space surveillance governance [17], emphasizing the importance of international legal cooperation and the establishment of transparent regulatory mechanisms.

6. Toward a post-structuralist approach in space cybersecurity

As the digital age continues to reframe space security, a need arises for a reassessment of traditional security frameworks to effectively address the multilayered and evolving threats characteristic of this era. The complexity encapsulating these challenges underscores the requirement for a more refined understanding and an adaptive approach to space security. A post-structuralist approach offers a promising pathway for reimagining space security early in this discourse. This theoretical framework emphasizes the deconstruction of traditional power structures, the interrogation of established narratives, and the exploration of the fluidity of power relations in the cyber and space domains. Post-structuralism's intrinsic critique of fixed meanings and identities facilitates a more flexible and comprehensive analysis of security challenges that transcend national boundaries and defy simplistic solutions. In the application of a post-structuralist framework to space security, there is an acknowledgment of the significance of examining how language, discourse, and power dynamics shape our comprehension of security threats and responses. This perspective encourages a critical evaluation of the assumptions underpinning current security practices and the exploration of alternative strategies that are more inclusive and adaptable to the rapidly changing technological landscape. Moreover, the incorporation of structuralist theory enriches our understanding by providing a contrast to post-structuralist critiques and fostering interdisciplinary dialog on space security

dynamics. Furthermore, a post-structuralist approach promotes a holistic understanding of the global nature of space security, recognizing the interconnectedness of all actors involved, from nation-states to private entities and international organizations. To this end, incorporating structuralist theory, as it highlights the underlying frameworks within which these power structures operate, provides a foundational contrast to the post-structuralist critique.

This theoretical framework emphasizes the deconstruction of traditional power structures, the interrogation of established narratives, and the exploration of the fluidity of power relations in the cyber and space domains. Post-structuralism's intrinsic critique of fixed meanings and identities facilitates a more flexible and comprehensive analysis of security challenges that transcend national boundaries and defy simplistic solutions [8, 9]. From the outset, the dialog between structuralist insights and post-structuralist critiques enriches our understanding of space security dynamics.

Exploring critical perspectives from theorists such as Michel Foucault and Jacques Derrida sheds light on the complex interplay between language, discourse, and power dynamics in shaping security responses. This perspective encourages a critical evaluation of the assumptions underpinning current security practices and the exploration of alternative strategies that are more inclusive and adaptable to the rapidly changing technological landscape. For instance, the analysis of space security discourses can unveil how certain threats are prioritized over others, reflecting broader geopolitical interests rather than an objective assessment of risks [34].

Furthermore, a post-structuralist approach promotes a holistic understanding of the global nature of space security, recognizing the interconnectedness of all actors involved, from nation-states to private entities and international organizations. This standpoint advocates for collaborative and multi-stakeholder strategies that transcend traditional power hierarchies, fostering a more equitable and effective governance of space activities [35].

Author details

Ulpia-Elena Botezatu* and Adrian-Victor Vevera
National Institute for Research and Development in Informatics—ICI Bucharest, Romania

*Address all correspondence to: ulpia.botezatu@ici.ro

IntechOpen

References

[1] Botezatu U. Smart cities: Linking cyber resilience to outer space security. In: Smart Cities International Conference (SCIC) Proceedings; Oct. 2023. Vol. 10. 2023. pp. 395-406

[2] Defense Intelligence Agency. Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion [online]. 2022. Available from: Challenges_Security_Space_2022.pdf [Accessed: April 18, 2024]

[3] Sangfor Technologies. Space Cybersecurity: Exploring Challenges, and Opportunities [Online]. 25 September 2023. Available from: https://www.sangfor.com/blog/cybersecurity/space-cybersecurity-exploring-challenges-and-opportunities [Accessed: February 10, 2024]

[4] Georgescu A, Botezatu U, Popa A, Popa S, Arseni S. Critical infrastructure dependency on space systems. In: "Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 1, "Mircea cel Batran". Constanta, Romania: Naval Academy Press; 2016

[5] Autolitano S. A Europe fit for the digital age: The quest for cybersecurity unpacked. IAI Papers. 2020;**20**(07):1-5

[6] Lévi-Strauss C. Structural Anthropology. New York: Basic Books; 1963

[7] de Saussure F. In: Bally C, Sechehaye A, editors. In Collaboration with the Albert Riedlinger. Translated by Wade Baskin,Course in General Linguistics. New York: Philosophical Library; 1916/1959

[8] Foucault M. Power/Knowledge: Selected Interviews and Other Writings, 1972-1977. New York: Pantheon Books; 1977

[9] Derrida J. Writing and Difference. Chicago: University of Chicago Press; 1978

[10] Buzan B, Wæver O, de Wilde J. Security: A New Framework for Analysis. Boulder, Colorado: Lynne Rienner Pub; 1998

[11] Hansen L, Nissenbaum H. Digital disaster, cyber security and the Copenhagen school. International Studies Quarterly. 2009;**53**:1155-1175

[12] Lakušić M, Baltezarevic I. National security and the challenges of the digital age. Megatrend Revija. 2022;**19**:145-154

[13] Smart W. Lessons Learned Review of the WannaCry Ransomware Cyber Attack. London, UK: NHS UK; 2018

[14] Cybersecurity and Infrastructure Security Agency. Cyber-Attack Against Ukrainian Critical Infrastructure [Online]. 20 July 2021. Available from: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [Accessed: February 10, 2024]

[15] White House. National Cyber Strategy of the United States of America. National Cybersecurity Strategy | ONCD | The White House [online]. 2018. [Accessed: April 18, 2024]

[16] European Commission. Shaping Europe's Digital Future: The EU's Cybersecurity Strategy for the Digital Decade [online]. The Cybersecurity Strategy | Shaping Europe's digital future. 2020 [Accessed: April 18, 2024]

[17] Hasin G. From "space law" to "space governance": A policy-oriented perspective on international law and

outer space activities. Journal of Space Law. 2023;**64**(2):385-430

[18] United Nations Office for Outer Space Affairs. Long-Term Sustainability of Outer Space Activities [Online]. Available from: https://www.unoosa.org/oosa/en/ourwork/topics/long-term-sustainability-of-outer-space-activities.html [Accessed: February 10, 2024]

[19] ITU. Global Cybersecurity Index [Online]. ITU; 2023. Available from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [Accessed: March 19, 2024]

[20] ITU. ITU Cybersecurity Activities [Online]. 2024. Available from: https://www.itu.int/en/action/cybersecurity/Pages/default.aspx [Accessed: March 19, 2024]

[21] United Nations. A/76/135—Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Note/by the Secretary-General. New York: United Nations; 2021

[22] United Nations. Fourth Committee, without a Vote, Approves Draft Resolution on Outer Space after Russian Federation's Late Withdrawal of Competing Text [Online]. Available from: https://press.un.org/en/2023/gaspd790.doc.htm [Accessed: October 27, 2023]

[23] Eriksson J, Giacomello G. Cyberspace in space: Fragmentation, vulnerability, and uncertainty. In: Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation. London: Routledge; 2022

[24] Martin A-S. Outer space, the final frontier of cyberspace: Regulating cybersecurity issues in two interwoven domain. Astropolitics. 2023;**21**(1):1-22

[25] European Space Policy Institute. Space, Cyber, and Defense: Nvigating Interdisciplinary Challenges. Vienna: ESPI; 2023

[26] Gorman S, Dreazen Y, Cole A. Insurgents Hack U.S. Drones [Online]. 17 December 2009. Available from: https://www.wsj.com/articles/SB126102247889095011 [Accessed: March 19, 2024]

[27] United Nations Institute for Disarmament Affairs. Electronic and Cyber Warfare in Outer Space. Geneva: UNIDIR; 2019

[28] ETH Zurich. The New Frontier of Space Militarization [Online]. 6 February 2023. Available from: https://css.ethz.ch/en/center/CSS-news/2023/12/the-new-frontier-of-space-militarization.html [Accessed: February 10, 2024]

[29] Botezatu U. Attempted cyber security of systems and operations in outer space: An overview of space-based vulnerabilities. Romanian Cyber Security Journal. 2023;**5**(1):67-76

[30] Bingen K, Johnson K, Young M. Space Threat Assessment. CSIS: Washington, DC; 2023

[31] Privacy International. Surveillance [Online]. 2018. Available from: https://privacyinternational.org/learn/surveillance [Accessed: March 19, 2024]

[32] Electronic Frontier Foundation. Surveillance Technologies [Online]. 2024. Available from: https://www.eff.org/issues/mass-surveillance-technologies [Accessed: March 19, 2024]

[33] Fontes C, Perrone C. Ethics of Surveillance: Harnessing the Use of

Live Facial Recognition Technologies in Public Spaces for Law Enforcement, Research Brief [Online]. TU Munich; 2021. Available from: https://ieai.mcts.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf [Accessed: March 19, 2024]

[34] Butler J. Gender Trouble: Feminism and the Subversion of Identity. New York: Routledge; 1990

[35] Deleuze G, Guattari F. A Thousand Plateaus: Capitalism and Schizophrenia. Minneapolis: University of Minnesota Press; 1987

Chapter 7

Perspective Chapter: AUKUS Pillar 2 – Technology, Interoperability, and Advanced Capabilities in the Evolving Trilateral Security Partnership

Chris J. Dolan

Abstract

The Australia-United Kingdom-United States (AUKUS) partnership is more than an agreement on nuclear propulsion submarines. In Pillar 2 of the agreement, AUKUS serves as an advanced technological accelerator premised on strategic collaboration, interoperability, and integration in the Indo-Pacific. Pillar 2 prioritizes advanced technologies and defense industrial capabilities in the trilateral partnership's strategic competition with China. This perspective chapter unpacks eight functional areas that comprise Pillar 2: hypersonic missiles and long-range weapons, artificial intelligence, undersea capabilities, advanced cybersecurity, quantum technologies, autonomous weapon systems, information sharing, and innovation. Measures of success are determined by AUKUS partners applying these to balance China. However, bureaucratic impediments and export controls, protecting information, intelligence, and communications, and future expansion of AUKUS challenge the trilateral partnership. However, AUKUS Pillar 2 has strong potential to strengthen interoperability and build confidence and trust in innovative solutions to emerging threats. Pillar 2 represents a new form of alliance-building with its focus on technological innovation and information sharing, flexibility, integration, and interoperability. The perspective in this chapter is that AUKUS is a strategically significant alliance that furthers collaboration, integration, and interoperability in advanced defense technologies and capabilities in deterring China and projecting international order.

Keywords: AUKUS, Pillar 2, defense capabilities, advanced technologies, functional areas, integration, interoperability, Indo-Pacific, China, strategic competition

1. Introduction

The Australia-United Kingdom-United States (AUKUS) defense partnership is more than a nuclear submarine deal. AUKUS has strategic significance in strengthening technological and security cooperation in maintaining a "free and

open Indo-Pacific" in response to China's rising influence in this vital strategic environment [1]. Pillar 1 is a major investment in Australia's nuclear submarines and will be built in Australia and designed by the U.S. Pillar 1 boosts Australia's maritime capabilities and enhances power projection in the Indo-Pacific region in response to China's military modernization. AUKUS is much more than a defense alliance premised on warfighting and deterrence; rather, AUKUS is a partnership designed to advance next generation defense capabilities and technologies in the intense geopolitical competition with China [2].

With Pillar 2, AUKUS partners will collaborate and invest in developing advanced military technologies to boost their own capabilities in ways that maintain their advantage over China's expanding military and technological assets. Pillar 2 expands the trilateral partnership into eight advanced technological areas ranging from hypersonic weapons to advanced autonomous systems and quantum technologies [3]. Put simply, the Pillar 2 focus on developing advanced technologies complements the Pillar 1 emphasis on supplying Australia with nuclear-powered submarines. Pillar 2 embraces the idea of an intense military and technological competition with China by investing dollars and pounds into next-generation military capabilities to ensure that the Indo-Pacific region is shaped by the open and rules-based international order. Pillar 2 transforms the trilateral partnership into a significant alliance premised on technological, military, and intelligence cooperation and collaboration.

However, AUKUS is not a formal treaty alliance with binding security commitments like NATO. There is nothing in AUKUS like an Article 5 collective security provision in the North Atlantic Charter [2, 4]. AUKUS is a flexible and informal defense arrangement centered on developing and sharing nuclear submarine capabilities (Pillar 1) and advanced technologies and defense capabilities (Pillar 2) [5]. AUKUS is not an Indo-Pacific NATO. Rather, it is a strategic alliance that places a premium on integration and collaboration on defense capabilities and technological advancements and information sharing in response to security challenges in the Indo-Pacific region that will restructure geopolitical dynamics well into the twenty-first century.

The purpose of this chapter is to assess the goals and objectives in Pillar 2 of AUKUS, identify consequences and challenges, and highlight areas of success and technological transformation. The success of Pillar 2 depends on trust and solidarity of the trilateral partnership in the implementation of capabilities [6]. Challenging mindsets on interoperability, communication, integration of weapons systems, and sharing advanced technological capacities is essential. As former Prime Minister of Australia Kevin Rudd stated, Pillar 2 should be a "seamless integration between defense industries" [7].

It will also depend on the extent to which the already close defense relationship between Australia, the U.K., and the U.S. can transform into a collaborative strategic and intense with China over the future of security in the Indo-Pacific region [8]. The development of a shared strategic culture and like-mindedness will facilitate this transformation. The three partners are taking China's rise seriously and committed to strategic competition; however, they must follow through. Pillar 2 is consequential in the race between AUKUS members and China over who gets to set the rules in the Indo-Pacific region [6]. That is, Pillar 2 is a technological accelerator for integrated defense capabilities that will maintain stability, deter China's expanding capabilities, enhance technological and defense cooperation, and boost industrial capacities in the production of defense-related technologies.

2. Overview of Pillar 2 objective and goals

The objective of Pillar 2 is to remain ahead of China in the strategic competition over advanced technologies and military capabilities in the Indo-Pacific region [3]. Issued through a joint declaration on September 15, 2021, AUKUS is designed to develop capabilities to "promote a free and open Indo-Pacific that is secure and stable" [9]. In the near term, Pillar 2 seeks to improve efficiencies in interoperability in command and control and electronic warfare. In the long term, the pillar commits the trilateral partnership to integrating eight functional areas in hypersonic weapons, artificial intelligence, cybersecurity, quantum technologies, undersea capabilities, electronic warfare, information sharing, and innovation [10].

Working groups will monitor and coordinate advancements in the eight functional areas. Working group members are comprised of ministerial officials, legislative representatives, defense contractors, and researchers from leading universities, among others, in the three member states [11]. The effectiveness of each group is premised on developing public-private partnerships and collaboration as well as research and development initiatives focusing on advanced defense capabilities. The challenge will be overcoming barriers to collaboration, intelligence sharing, and adjusting export controls and regulations that could inhibit integration of technological capacities and weapons systems [12].

Each government is committed to supporting the defense capabilities and national security posture of the other by enhancing existing trilateral military capacities in the Indo-Pacific region [13]. Activities are coordinated through each working group. Developments in functional areas will be determined by combining intelligence sharing and partnerships, technological collaboration, innovation and scientific capacities, and integration of procurement, supply chains, and defense industrial bases [12].

While empirical research and theory on AUKUS is emerging and evolving, the academic literature focusing on Pillar 2 remains underdeveloped. Scholarly assessments of Pillar 2 are crucial to understanding technological and military competition with China as the race for critical technologies is fast becoming a pivot point for innovation in artificial intelligence and machine learning, semiconductors, and biotechnology. Fraser and Solomon explain that ad hoc alliances like AUKUS and the Quadrilateral Security Dialogue (the Quad) function as "minilaterals" that have the potential to reshape the "Indo-Pacific security architecture" given their focus on collaboration in "defense-technology" [14]. Taylor further develops this approach by observing that the parameters of Pillar 2 rest on concepts of integration, collective deterrence, and innovation power advanced defense technologies undergird AUKUS as "a minilateral institutional arrangement" [15]. But as Cheng maintains, the as technological and military advancements unfold, AUKUS is likely to provoke China as it "will have no choice but keep elevating their military levels" [16].

Leoni and Tzinieris argue that the strategic focus on technological elements allow AUKUS to function as a coalition-building project through a world order studies perspective [17]. Koga takes this one step further by observing that coalition-building efforts made possible by AUKUS, and the Quad reflect "tactical hedging," in which the three like-minded partners share similar interests in coordinating efforts to contain China's rising military and economic influence [18]. Another study suggests that AUKUS Pillar 2 should be understood as central to upholding a "free and open Indo-Pacific" that can include additional partners like Canada, New Zealand, Japan, and India [19]. However, Tzinieris, Chuahan, and Athansiadou argue that contrary to

U.S. efforts to align with India more closely, New Delhi has no intention of ceding its "strategic autonomy" [20].

The methodological or conceptual perspective of this chapter is premised on integration, interoperability, and collaboration in the prioritization of advanced technological assets among the three AUKUS partners in Pillar 2. Australia, U.K., and U.S. are sharpening their focus on applying advanced capabilities and maintaining their technological edge in response to major power adversaries, especially China. President Biden has described China's rise and investments in military technologies as a challenge to the "current strategic environment" [1]. Therefore, Pillar 2 is designed to develop solutions for this competition over who gets to set the rules in the Indo-Pacific and determine regional security. While China objected to AUKUS an effort to contain its rise and influence in Asia, most states in the Indo-Pacific region have quietly, cautiously, or enthusiastically supported the defense arrangement or have not expressed an objection or opinion [21].

Progress will be determined by investments made in joint projects in the eight functional areas. For example, in quantum technologies, an "AUKUS Quantum Arrangement" was created boost "generation-after-next quantum capabilities" in defense integration of navigation, positioning, and timing technologies by 2026 [22, 23]. A "Trade Authorization Mechanism" will modernize collaborative efforts in "technology sharing and defense trade among only the AUKUS partners" [24]. While Pillar 2 makes significant investments in military partnerships for AUKUS members, success will be determined by overcoming standard operating procedures in defense and established mindsets on sharing advanced technologies as well as the geopolitical realities of competing with China in the Indo-Pacific.

3. Functional areas

Pillar 2 has targeted eight areas in which member states will invest and advance military and technological capabilities. This section will explain each area and assess challenges and opportunities.

3.1 Hypersonic missiles

Pillar 2 supercharges research and development and deployment of hypersonic missiles that close the reaction times of air defense systems and threaten targeted sites. Integration among AUKUS members means that the three members will carry tremendous and decisive advantages in the Indo-Pacific and serve as a major deterrent to China in the region [25]. Given that these weapons fly at the speed of Mach 5 or higher, the potential to alter the complex balance of power in the Indo-Pacific by checking China's prompt acceleration of these technologies [26].

The incredible speed, maneuverability, and precision of hypersonic missiles make them a priority weapon in the AUKUS arsenal. Put simply, the development of hypersonic missiles and integration within trilateral defense will provide AUKUS with a decisive strategic advantage. The accuracy of these weapons, high precision capabilities, and advanced platforms will minimize collateral damage and offer flexible response [27].

The dedicated working group on hypersonic missiles focuses on research and development, technology transfers, and information sharing. Facilitating joint projects depends on integrating existing hypersonic programs [21, 22]. Australia's

High-Speed Projectile hypersonic project is currently being developed by BAE Systems Australia as "Project Javelin" under the supervision of Defence Australia and aligned with the 2020 Force Structure Plan that dedicates $30 billion in high-speed weapons systems and other programs [28]. The U.S. is investing in hypersonic glide vehicles that utilize kinetic energy to fly at high speed and cruise missiles powered by scramjets [29]. The U.K. will likely purchase glide vehicles through its partnership in AUKUS as well as investing in advanced hypersonic development projects as it does not possess a program [30, 31].

Over the next several years, AUKUS partners will test and assess the effectiveness of these programs and accelerate development and deployment. While AUKUS is committed to program integration, these projects are costly and could pose logistical hurdles [23]. Ensuring a steady stream of public and private R&D investments and overcoming technical and operational difficulties in the weapons systems will challenge partner states [22]. More important, while hypersonic weapons are a powerful deterrent against aggressors, long-range capabilities may complicate arms control initiatives and lead to weapons proliferation in the Indo-Pacific with China, Russia, and North Korea pursuing and sharing their own capabilities [27]. The risks are apparent and the prospects for escalation are high as hypersonic capabilities increase.

3.2 Artificial intelligence

Given the complexities and rapid change in artificial intelligence and machine learning technologies, AUKUS has prioritized infusion of AI systems within defense capabilities. The goal is to apply AI in ways that enhance targeting across conventional military, information, and cyber domains in a responsible fashion [32, 33]. Effective AI can process and assess data in rapid and efficient ways and assist with integrated assessments of patterns and trends in the threat landscape [34]. Furthermore, it can enhance procurement and supply chains, training on weapons systems, and logistics [22]. AI will also improve autonomous weapons like drones, covert operations, and reconnaissance as well as AI-enabled tools for improving critical infrastructure protection of integrated defense industrial bases [35, 36].

Before AUKUS was announced in September 2021, Australia, the U.S., and U.K. had already developed comprehensive AI-powered security tools and autonomous systems [22]. The U.S. Joint Artificial Intelligence Center manages AI applications in each military branch with "mission initiatives" in health and business processes, joint logistics, joint force protection, joint information warfare, academic/industry engagement, and joint command and control [22, 37]. In 2023, the U.S. defense budget allocated $5 million for an "Artificial Intelligence development Hub" under the category of "AUKUS Innovation Initiatives" [38–41]. In 2021, Australia released "Australia's AI Action Plan" and one year later the U.K. Ministry of Defence developed a "Defence Artificial Intelligence Strategy" [41].

However, AI presents many challenges. Integrating three AI systems in three militaries will be difficult especially as it relates to developing pipelines of talent into defense departments and ministries and retaining personnel [42]. Another challenge will be to ensure that AI-systems are not subject to biases that can infect data processing, collections, and analysis [23]. In addition to responsible use of AI-enabled tools, instilling transparency into military systems will be consequential for integration and interoperability. As much as integration is a challenge in AI capabilities, concerns about oversight and lack of human control are considerations in building a trilateral culture of responsible use of autonomous systems [43].

3.3 Quantum technologies

This functional area puts forth an "AUKUS Quantum Arrangement" that invests in quantum computing in communications and cryptography. The Arrangement coordinates American, Australian, and British innovation and research and development in navigation and timing for global positioning systems across domains [44]. These initiatives are designed to secure communications and enhance critical infrastructure resilience activities through cryptography, cybersecurity, and encryption [45]. Quantum sensors will enhance precision timing and positioning for targeting and navigation in operations, computer simulations, wargaming, logistics, and weapons, and improve signals and imagery intelligence collections [23].

Initiatives developed through the arrangement are based on the U.S. Defense Quantum Information Science and Technology Research and Development Program [46]. This initiative came into effect in 2019 to invest in R&D for quantum science R&D and promote interagency communication within the Department of Defense. Similar measures have been undertaken in Australia and the U.K. to boost collaboration in R&D in quantum technologies [22].

The Quantum Arrangement presents both opportunities and risks for AUKUS [43]. The arrangement is expected to enhance intelligence collections and sharing, attract talent through recruitment and research investments, and collaboration on networks, cryptography, and sensors [47]. However, if investments are not sustainable over the long term, technological challenges are bound to arise. Expert talent could be lost to other industries with higher compensation and regional security could be at risk if a quantum arms race with China and Russia ensues. Moreover, in the absence of strong governance and ethical guidelines, data leaks, and misuse of simulations and wargaming could destabilize the balance of power in the Indo-Pacific [22].

3.4 Advanced cybersecurity

Increasing collaboration on cyber defense measures and integrating and boosting offensive cyberwar capabilities and threat intelligence is a key element in Pillar 2 [22, 23]. The importance of integration and information sharing in multi-domain operations in an irregular warfare context will shape strategic competition with China and Russia. The ability to wage contemporary cyberwarfare against these adversaries depends on secure IT systems and critical infrastructure in key sectors like energy, defense industrial bases, telecommunications, financial institutions, health care, and transportation [48].

Cyberattacks from malicious state or non-state actors could disrupt networks and spread through critical sectors, crippling financial systems, destabilizing governments, and dislocating social life. The SolarWinds Hack in 2020 was a devastating supply chain attack and the Colonial Pipeline ransomware attack disrupted U.S. energy distribution as did the Microsoft Exchange attack [49]. Australia suffered several damaging cyberattacks such as the platform Canva, Optus telecommunications, and the data breach at Latitude financial services [50]. Devastating cyber incidents against the U.K. targeted the Manchester police in a series of ransomware attacks in 2023 [51].

AUKUS partners have relatively robust national cybersecurity strategies that put forth similar goals and objectives in cyber defense and critical infrastructure protection [22]. The 2023 U.S. Cyber Security Strategy advances five priorities:

securing and protecting privacy in America's 16 critical infrastructure sectors; dismantling malicious threat actors; public-private partnerships for recovery and resilience; research and development in cyber technologies; and building international partnerships and arrangements [52].

Australia and the U.K. have similar strategic goals that highlight the importance of resilience and collaboration between national defense agencies and commercial entities. Australia's National Cyber Security Strategy of 2023 to 2030 advances similar themes of protecting businesses and citizens, protecting technology, threat sharing, critical infrastructure, sovereign capabilities, and global leadership. This was supplemented with an action plan highlighting the importance of collaborating with the private sector to develop new and advanced cyber technologies for critical infrastructure resilience [53]. Similar to the U.S. and Australia, the U.K.'s 2022 national Cyber Security Strategy rests on making investments in industry and universities; data protection and digital prosperity; industrial capabilities and secure cyber technologies for critical infrastructure; shaping international cyber norms; and public-private partnerships [54].

The overlapping themes in cybersecurity strategies among AUKUS partners shows that modern warfare is interconnected and reliant on secure critical infrastructure and information technology/operational technologies. Collaboration within AUKUS is focused on sharing compliance guidelines and best practices, joint protocols for incident response, and enhancement of offensive cyberwarfare techniques [43]. Protecting critical infrastructure sectors from cyberattacks against electrical grids, transportation systems, banks, hospitals, wastewater treatment, commercial services, defense production, and mobile networks are now national security priorities. Cyber defense integration within AUKUS means collaboration and merging approaches to attracting and retaining professional cybersecurity talent, cyber professional development, training, and public awareness about data protection and privacy [35]. Successful integration involves holding joint cyber exercises, vulnerability scanning, penetration testing, risk mitigation, sharing real-time threat intelligence and information, and partnerships with private sector businesses and academia.

AUKUS confronts several challenges in integrating cyber defense measures. The trilateral partnership should consider developing and uphold cyber norms that hold malicious threat actors accountable and focuses on attribution of cyber incidents. Merging vulnerability scanning, risk assessment, and threat intelligence to delineate trends in the threat landscape will involve integration of artificial intelligence and machine learning capabilities [43]. This raises the possibility of new vulnerabilities that could be exploited by malicious threat actors. The focus on integrated cyber defense suggests that cybersecurity is crucial to defending battlespaces and critical infrastructure through workforce development, talent recruitment and retention, collaboration with the private sector, and R&D [22, 23].

3.5 Undersea capabilities

Within AUKUS, undersea capabilities refer to unmanned high technology military systems which operate underwater for robotic and other purposes. For the U.S. Navy, the focus is on R&D efforts on procurement and operation of unmanned underwater vehicles (UUVs) and other advanced systems that differ in size and capability and have intelligence collections capabilities, advanced sensors for tracking movements, reconnaissance, anti-mining capacities and countermeasures, anti-submarine and anti-surface capabilities, and can maintain communications networks [55]. The

U.K. Royal Navy purchased and acquired REMUS unmanned vehicles and the Royal Australian Navy has partnered with defense corporations for larger Speartooth undersea vehicles and systems [55–58].

Coordination and integration of undersea capabilities among the U.S. Navy, Royal Navy, and Royal Australian Navy takes place through the AUKUS Undersea Capabilities Working Group [23]. The group established the AUKUS Undersea Robotics Autonomous Systems initiative, which is developing small to larger and long range autonomous undersea vehicles [59]. According to the White House, the initiative will serve as "a significant force multiplier for [AUKUS] maritime forces" with $10 million allocated to for unmanned undersea mission payloads and another $25 million for "AUKUS Innovation Initiatives." Australia partners with the American defense technology company Anduril Industries for delivery of extra-large autonomous undersea vehicle prototypes to the Royal Australian Navy [60, 61].

To maintain a free and open waterways and maritime security through key chokepoints, advanced unmanned undersea robotic capabilities are of vital strategic importance to AUKUS. Integrated unmanned underwater vehicle systems will enhance interoperability, communications with submarines, and early detection of threats [62]. China's development of undersea capabilities and technologies could alter the balance of power in the Indo- Pacific and threaten the underwater environment [63].

However, new investments and developing undersea capabilities come with several challenges and risks. Advanced underwater military and intelligence technologies are complex, sophisticated, and come with a hefty price tag in national R&D budgets [62]. These are highly sensitive vehicles that operate in tough and challenging underwater environments and will face China's rapidly advancing undersea vehicles [64].

A strong AUKUS undersea presence can serve two purposes. First, unmanned underwater vehicles function as an effective deterrent to China and other adversaries threatening naval operations or commercial shipping. Second, AUKUS could enhance scientific progress in civilian oceanographic research and undersea exploration [22, 23].

3.6 Electronic warfare

Development of advanced technologies to attack or undermine adversary communications and radar comprises electronic warfare (EW). EW systems present AUKUS with considerable tactical advantages as next-generation capabilities allow partners to exploit the electromagnetic spectrum to blind radars, disrupt GPS navigation and deceive adversaries, and, should it become necessary, launch attacks on targeted sites [65]. Strong countermeasures also allow AUKUS partners to build critical infrastructure resilience in civilian and military systems [66]. Also, EW systems allow more effective and covert intelligence collections using electronic and communications signals, boosting early detection and threat intelligence of adversary patterns and trends over time [67]. Moreover, AUKUS's EW capacities will help counter China's EW systems.

AUKUS integration of EW systems involves merging defense platforms for drones, warships, warplanes, and fixed ground-sites. To optimize integration and ensure continuous interoperability while mitigating risks, joint exercises will take place simulating coordinated electronic attacks and enhanced electronic defenses [22, 23]. The integration process will be assisted by the fact that Australia, the U.K, and U.S.

operate the U.S. Air Force AEW&C E-7 Wedgetail platform [68]. The platform integration advantage boosts battlefield and battlespace dominance while protecting Australian, British, and American forces in the Indo-Pacific [69].

Given rapid advances in communications, radar systems, and GPS navigation, remaining ahead of China demands uninterrupted government and private sector investments in R&D to update EW systems [70]. Cybersecurity must also be regularly updated, and networks patched given that vulnerabilities will be exploited by adversaries. Vulnerability scanning and risk mitigation should be incorporated into integration processes to minimize unintended consequences.

3.7 Information sharing

Collaboration and cooperation on critical information is so important in AUKUS that it has been provided its own specific functional area in Pillar 2. Information sharing is concerned with building secure mechanisms and systems for sharing sensitive data and classified information on military technologies, weapons systems, and interoperability among cleared personnel in the trilateral partnership [71]. Effective information sharing involves maintaining mutual confidence and assurance while also strengthening defense posture in the intensely competitive Indo-Pacific.

Sharing and using classified information and data is the foundation upon which AUKUS will function as a meaningful trilateral partnership. Put simply, confidence and trust undergird AUKUS pillars 1 and 2. Australia, the U.K., and U.S. already have a history of trusted cooperation and information sharing in the Five Eyes intelligence partnership that also includes Canada and New Zealand [72]. The role of advanced technologies in hypersonic missiles systems, undersea capabilities, cybersecurity, artificial intelligence, quantum technologies, electronic warfare, and innovation rests on enhanced collaboration driving benefits derived from shared expertise among AUKUS forces [5]. Collecting and sharing information drives cooperation on integrated and joint operations in response to threats, risks, and vulnerabilities in the Indo-Pacific [73].

The information sharing working group will develop secure communications to facilitate integration of intelligence and defense capabilities across functional areas. A secured cloud will allow for joint access among cleared personnel to move AUKUS forward on integrated intelligence collections and analysis and information sharing on hypersonic missiles, cybersecurity, artificial intelligence, quantum technologies, undersea capabilities, innovation, and electronic warfare [74]. Secure sharing of classified intelligence and data exchanges are determined by common security standards and procedures developed in the working group [75].

However, the risks of intelligence sharing are significant as potential vulnerabilities could expose AUKUS to malicious state and non-state actors seeking to penetrate secure systems and gain access to classified information and data [22]. Striking the appropriate balance between sharing information on advanced defense technologies and securing classified intelligence through common security systems to prevent unauthorized access is vital to AUKUS [76]. Also, addressing differences in security clearance processes and data platforms is paramount. Effective information sharing comes down to trust and confidence as well as transparency among the three partners.

Barriers to information sharing, such as restrictive export controls and bureaucratic politics premised on long established standard operating procedures and risk aversion on controlled classified intelligence, will impede integration and interoperability [77]. Some experts including American legislators have argued that

existing U.S. export controls could obstruct information sharing about advanced technologies and defense industrial capacities with Australia and the U.K. U.S. defense regulations and procedures could impose undue burdens and prevent defense contractors from pursuing joint defense projects and delay implementation [78–80].

3.8 Innovation

While trust and confidence are essential for information and intelligence sharing, innovation is consequential for AUKUS to maintain its strategic advantage in the security environment and threat landscape in the Indo-Pacific [81–83]. Innovation will be driven by collaborative investments and personnel driving joint research and development initiatives in next-generation technologies, diverse software applications, and hardware in support of defense capabilities [23, 71, 76]. Pooled R&D resources will determine the extent of innovation and scientific capacities. Innovation could even stimulate dual-use applications and specific technological advancements for commercial enterprises and consumers [84, 85].

Collaborative innovation among AUKUS partners will also be shaped by a toleration for risk taking and flexibility. Investing and funding in both established multinational corporations and startups will help sustain an integrated and dynamic scientific ecosystem [42]. Incentives for building and maintaining public-private partnerships will encourage knowledge-sharing and extend the defense workforce into other domains. In December 2023, AUKUS defense leaders announced the creation of an "innovation challenge series" that would encourage participation from the private sector on new ways to develop electronic warfare capabilities [86].

Australian, British, and American companies will drive innovation among AUKUS partners, allowing it to maintain and expand its strategic edge in the intense competition with China in the Indo-Pacific [23, 87]. With the integration of the three private industries in AUKUS countries there is a strong likelihood for rapid new initiatives in artificial intelligence and machine learning, autonomous platforms, underwater detection, materials science, propulsion, and global positioning [42].

But there are challenges that could withhold the pace of innovation. First, recruiting and retaining qualified personnel and expertise who could obtain higher compensation packages in other industries will be a major challenge [88]. Second, there are questions about guaranteeing ethical and responsible use of new and next-generation technologies, especially those that relate to artificial intelligence and machine learning tools as well as autonomous weapons [89]. Although the advantages of such capabilities include enhanced data analysis, stronger situational awareness, automated defense and intelligence tasks, and improved cybersecurity, lack of transparency and misuse of autonomous weapons for offensive purposes, and privacy concerns could arise. Third, common security procedures and protocols must ensure that rapid advancements in innovative defense technologies do not elevate speed over security. The need to maintain standards, best practices, and compliance should keep up with the rapid pace of innovation in functional areas like AI-enabled defense capabilities [89].

4. Conclusions

AUKUS is a trilateral security partnership developed in response to the rising significance of the Indo-Pacific region and China's expanding influence. Pillar 2 is

important given its focus on integration of defense capabilities and advanced technological collaboration in hypersonic missiles and long-range weapons, artificial intelligence, undersea capabilities, advanced cybersecurity, quantum technologies, autonomous weapons systems, information sharing, and innovation. New and emerging security threats in the Indo-Pacific led to the formation of the functional areas on integration and interoperability in AUKUS Pillar 2 [90]. However, the eight areas are abstract with a lot of programs, products, public institutions, and private entities involved in shaping technologies and defense capabilities. The diverse array of areas and existing export controls could present bureaucratic impediments to joint projects and exercises [91].

Overcoming the challenges of integrating defense technologies and capabilities requires a significant diplomatic effort in the three AUKUS partners [92]. AUKUS partners must put resources into balancing strategic competition with China in the Indo-Pacific while communicating and collaborating with one another. Also, hypersonic weapons and long-range weapons systems risk escalation with China, Russia, and North Korea. Furthermore, information and intelligence sharing of advanced technologies and defense assets among AUKUS partners demands security controls to prevent data leaks, breaches and incidents, and cyber espionage. Supercharging artificial intelligence, cybersecurity, and autonomous weapons should raise serious concerns about privacy, bias, and abuse. AUKUS partners must adhere to ethical principles and responsible use.

Unlike NATO, it is a flexible partnership with less formal impediments for developing partnerships and including new members. Pillar 2 offers considerable opportunities for non-nuclear partners interested in building technological and defense capabilities. Canada and New Zealand are more likely to partner with AUKUS Pillar 2 given they are already in the Five Eyes intelligence sharing compact [93, 94]. New Zealand could be enticed given geostrategic realities. Defence Minister Andrew Little stated, that if New Zealand was offered access to Pillar 2 areas, it was "willing to explore it" [95, 96]. In May 2023, it was reported that Canada may be interested in entering Pillar 2 areas to boost its artificial intelligence and cybersecurity capabilities [97, 98]. Japan is also another potential AUKUS Pillar 2 partner given its defense industrial and technological relationship with the U.S. and concerns about China [99].

AUKUS Pillar 2 is an endeavor premised on developing collaboration and integration. The opportunities for integration of advanced technologies and next-generation defense capabilities are extensive and substantial. The trilateral partnership is serious about pooling R&D and expertise to develop technologies that will provide AUKUS partners with a strategic edge over China in the Indo-Pacific [2, 6, 23].

Deeper integration of cutting-edge technologies will boost joint operations and enhance the ability of three partners to promote a rules-based order in the face of adversaries seeking to upend them [3, 6]. The commitment to responsible use and transparency will be defining features of the partnership. With Pillar 2, deeper connections among the defense assets of the three partners will strengthen collaboration and interoperability. AUKUS is unlike other alliance systems, namely NATO, in that it is a flexible and capabilities-based partnership driven by confidence and trust, accelerated innovation, and knowledge and information sharing [2, 4].

Author details

Chris J. Dolan
Intelligence and Security Studies, Lebanon Valley College, United States

*Address all correspondence to: dolan@lvc.edu

IntechOpen

References

[1] Wintour P. What is the AUKUS alliance and what are its implications? The Guardian. 2021. Available from: https://www.theguardian.com/politics/2021/sep/16/what-is-the-aukus-alliance-and-what-are-its-implications

[2] Bassi J, Ryan M, Curtis L. AUKUS is more than submarines. Its advanced capabilities pillar will also require fundamental shifts. Just Security. 10 Jul 2023. Available from: https://www.justsecurity.org/87195/aukus-is-more-than-submarines-its-advanced-capabilities-pillar-will-also-require-fundamental-shifts/

[3] Townshend A. The AUKUS submarine deal highlights a tectonic shift in the US Australia alliance. Carnegie Endowment for International Peace. 2023. Available from: https://www.carnegieendowment.org/2023/03/27/aukus-submarine-deal-highlights-tectonic-shift-in-u.s.-australia-alliance-pub-89383

[4] Jennings P. AUKUS: New opportunities for the United States and its closest allies. Heritage Foundation. 2022. Available from: https://www.heritage.org/military-strength/topical-essays/aukus-new-opportunities-the-united-states-and-its

[5] Sevasopulo D, Rachman G, Pfeifer S. White House optimistic on tech sharing for AUKUS security pact. Financial Times. 2023. Available from: https://www.ft.com/content/51d4d996-8adf497a-a07b-b257067d0739

[6] Kahn L. AUKUS explained: How will the trilateral pact shape Indo-Pacific Security? Council on Foreign Relations. 2023. Available from: https://www.cfr.org/in-brief/aukus-explained-how-will-trilateral-pact-shape-indo-pacific-security

[7] A conversation with Ambassador Kevin Rudd, Australia's New Ambassador to the United States. Center for Strategic and International Studies. 2023. Available from: https://www.csis.org/analysis/conversation-ambassador-kevin-rudd-australias-new-ambassador-united-states

[8] Carouso J, Schieffer T, Bleich J, Berry J, Culvahouse A. ITAR should end for Australia. Center for Strategic and International Studies. 2022. Available from: https://www.csis.org/analysis/itar-should-end-australia

[9] Joint Leaders Statement on AUKUS. The White House, 2023. Available from: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/13/joint-leaders-statement-on-aukus-2/

[10] Burke J. No headlines, but AUKUS part two just as important. The Australian. 2023. Available from: https://www.theaustralian.com.au/subscribe/news/1/?sourceCode=TAWEB_WRE170_a&dest=https%3A%2F%2Fwww.theaustralian.com.au%2Fcommentary% 2Fno-headlines-but- aukus-part-two-just-as-important%2Fnews-story%2F69b63aaf5ae99cda9368f7f7 f226eee3&memtype=anonymous&mode=premium&v21=GROUPB-Segment-1-NOSCORE&V21spcbehaviour=append

[11] Detsch J, Gramer R. Biden's AUKUS point man to exit. Foreign Policy. 2023. Available from: https://www.foreignpolicy.com/2023/03/10/biden-aukus-miller-us-uk-australia-china-france/

[12] Corben T, Greenwalt W. Breaking the barriers: Reforming US export controls to realise the potential of AUKUS. United States Studies Centre. 2023. Available

from: https://www.ussc.edu.au/breaking-the-barriers-reforming-us-export-controls-to-realise-the-potential-of-aukus

[13] Townshend A, Feigenbaum E, Pettyjohn S, Greenwalt W. Making AUKUS work for the U.S.-Australia alliance [video]. Carnegie Endowment for International Peace. 2023. Available from: https://www.carnegieendowment.org/2023/03/16/making-aukus-work-for-u.s.-australia-alliance-event-8052

[14] Fraser J, Soliman M. The Quad, AUKUS, and I2U2 formats: Major lessons from minilaterals. Orbis. 12 Jul 2023;**67**(3):411. Available from: https://www.fpri.org/article/2023/07/the-quad-aukus-and-i2u2-formats-major-lessons-from-minilaterals/

[15] Taylor M. AUKUS, Advanced Capabilities and Defense Integration in the Indo-Pacific. Issue and Policy Briefs. University of Helsinki; 2023. pp. 1-9. Available from: https://www.researchportal.helsinki.fi/en/publications/aukus-advanced-capabilities-and-defense-integration-in-the-indo-p

[16] Cheng M. AUKUS: The changing dynamic and its regional implications. European Journal of Development Studies. 3 Feb 2022;**6**. Available from: https://www.ej-develop.org/index.php/ejdevelop/article/view/63/24

[17] Leoni Z, Tzinieris S. To exclude or not to exclude: AUKUS and order-engineering. Security and Defence. 2023. Available from: https://www.securityanddefenceplus.plusalliance.org/essays/to-exclude-or-not-toexclude-aukus-and-order-engineering/

[18] Koga K. Tactical hedging as coalition-building signal: The evolution of the quad and AUKUS in the Indo-Pacific. British Journal of Politics and International Relations. 2024. Available from: https://www.journals.sagepub.com/doi/full/10.1177/13691481241227840

[19] Vucetic D. Guest editor's introduction: AUKUS among democracies. Contemporary International History. 29 Aug 2023;**78**(3):293-306. Available from: https://journals.sagepub.com/doi/10.1177/00207020231198134

[20] Tzinieris S, Chuahan R, Athansiadou E. India's A La Carte minilateralism: AUKUS and the quad. The Washington Quarterly. 2023;**66**(4):21-39

[21] Rachman G. Why AUKUS is welcome in the Indo-Pacific. The Financial Times. 2021. Available from: https://www.ft.com/content/cac4b3b0-faec-4648-a49d-8dbcd96eac02

[22] Parrish P, Nicastro L. AUKUS Pillar 2: Background and issues for congress. Congressional Research Service, R47599. 2023. Available from: https://www.crsreports.congress.gov/product/pdf/R/R47599

[23] Christianson J, Monaghan S, Cooke D. AUKUS pillar two: Advancing the capabilities of the United States, United Kingdom, and Australia. Center for Strategic and International Studies. 2023. Available from: https://www.csis.org/analysis/aukus-pillar-two-advancing-capabilities-united-states-united-kingdom-and-australia

[24] House Foreign Affairs Committee Hearing on Modernizing U.S. Arms Exports and a Stronger AUKUS. 2023. Available from: https://www.foreignaffairs.house.gov/hearing/modernizing-u-s-arms-exports-and-a-stronger-aukus/

[25] Brooke-Holland L. AUKUS Pillar 2: Advanced Capabilities Programmes.

House of Commons Library. 2023. Available from: https://www.researchbriefings.files.parliament.uk/documents/CBP-9842/CBP-9842.pdf

[26] Sayler KM. Hypersonic Weapons: Background and Issues for Congress. CRS Report R45811. 2023. Available from: https://www.crsreports.congress.gov/product/details?prodcode=R45811

[27] Sevastopulo D, Rathbone JP, Fildes N. Joe Biden Announces US, UK, and Australia co-operation on hypersonic weapons. Financial Times. 2022. Available from: https://www.ft.com/content/b8ddf153-b9ca-4db5-8835-cb8509a9921f

[28] Project Javelin Aims to Build Australian Hypersonic Missile by 2025. Australian Defence Magazine. 2023. Available from: https://www.australiandefence.com.au/defence/joint/project-javelin-aims-to-build-australian-hypersonic-missile-by-2025

[29] Osborn K. How one scramjet changed the hypersonic weapons showdown. The National Interest. 2021. Available from: https://www.nationalinterest.org/blog/buzz/how-one-scramjet-changed-hypersonic-weapons-showdown-194637

[30] Allison GUK. Confirms it is accelerating hypersonic weapons project. UK Defence Journal. 2022. Available from: https://www.ukdefencejournal.org.uk/uk-confirms-it-is-accelerating-hypersonic-weapon-project/

[31] Cooney C. Hypersonic missiles: UK, US, and Australia to boost defence co-operation. BBC News. 2022. Available from: https://www.bbc.com/news/uk-61000416

[32] Jackett J. Laying the foundations for AUKUS: Strengthening Australia's high-tech ecosystem in support of advanced. United States Studies Centre. 2022. Available from: https://www.ussc.edu.au/strengthening-australias-high-tech-ecosystem-in-support-of-advanced-capabilities

[33] Hoffman W. AI and the future of cyber competition. Center for Security and Emerging Technology. 2021. Available from: https://www.cset.georgetown.edu/publication/ai-and-the-future-of-cyber-competition/

[34] Hay Newman L. NSA Cybersecurity Director Says "Buckle Up" for Generative AI. Wired. 2023. Available from: https://www.wired.com/story/nsa-rob-joyce-chatgpt-security/

[35] Barrett T, Mayo S. AUKUS status update: Checking in on the advancement of pillar II. United State Studies Centre. 2023. Available from: https://www.ussc.edu.au/aukus-status-update-checking-in-on-the-advancement-of-pillar-ii

[36] Lohn A, Knack A, Burke A, Jackson K. Autonomous cyber defense: A roadmap from lab to ops. Alan Turing Institute. Center for Emerging Technology and Security. 2023. Available from: https://www.cetas.turing.ac.uk/publications/autonomous-cyber-defence

[37] Van der Schyff J. AUKUS will redefine government–industry partnerships. The Strategist. 2023. Available from: https://www.aspistrategist.org.au/aukus-will-redefine-government-industry-partnerships/

[38] U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway. 2022. Available from: https://www.media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-ResponsibleArtificial-Intelligence-Strategy-and-Implementation-Pathway.pdf

[39] Theohary, CA. CRS In Focus: Defense Primer: Cyberspace Operations. Congressional Research Service, IF10537, December 14, 2023: https://www.sgp.fas.org/crs/natsec/IF10537.pdf

[40] Defence Artificial Intelligence Strategy. UK Ministry of Defence. 2022. Available from: https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy

[41] Australia's AI Action Plan. Australian Government. 2021. Available from: https://www.webarchive.nla.gov.au/awa/20220816053410/https://www.industry.gov.au/data-andpublications/australias-artificial-intelligence-action-plan

[42] Wyatt A, Ryseff J, Yoshiara E, Bondreaux B, Black M, Black J. Towards AUKUS Collaboration on Responsible Military Artificial Intelligence. RAND. 2024. Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3000/RRA3079-1/RAND_RRA3079-1.pdf

[43] Luckenbaugh J. Just in: AUKUS partners advancing on AI. Autonomy. National Defense Magazine. 2023. Available from: https://www.nationaldefensemagazine.org/articles/2023/9/20/aukus-partners-advancing-on-ai-autonomy

[44] Saylor KM. Defense primer: Quantum technology. Congressional Research Service, IF11836. 2023. Available from: https://www.crsreports.congress.gov/product/pdf/IF/IF11836

[45] 1.5 – Fact Sheet: Implementation of the AUKUS Partnership. Security and Defence Plus, 2022. Available from: https://www.securityanddefenceplus.plusalliance.org/wp-content/uploads/2022/08/Fact-Sheet-Implementation-of-the-AUKUS-Partnership.pdf

[46] GAO. Quantum technologies: Defense laboratories should take steps to improve workforce planning. Government Accountability Office. 2023. Available from: https://www.gao.gov/assets/d24106284.pdf

[47] Munro B, Paci T. AUKUS must focus on quantum policy, not just the technology. Australian Strategic Policy Institute: The Strategist. 2023. Available from: https://www.aspistrategist.org.au/aukus-must-focus-on-quantum-policy-not-just-the-technology/

[48] Poireault K. UK discloses offensive cyber capabilities principles. Information Security Magazine. 2023. Available from: https://www.infosecurity-magazine.com/news/uk-offensive-cyber-capabilities/

[49] Thompson T. The colonial pipeline ransomware attack and the solarwinds hack were all but inevitable: Why cyber defense is a wicked problem. The Conversation. 2021. Available from: https://www.theconversation.com/the-colonial-pipeline-ransomware-attack-and-the-solarwinds-hack-were-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-160661

[50] Doran M. China blamed as major backer behind hacking of Australian companies and infrastructure. ABC Net. Available from: https://www.abc.net.au/news/2023-11-15/asd-reports-increase-in-cyber-attacks/103103320

[51] Milmo D. Who is behind the latest wave of U.K. ransomware attacks? The Guardian. 2023. Available from: https://www.theguardian.com/technology/2023/sep/14/who-is-behind-latest-wave-of-ransomware-attacks

[52] National Cyber Security Strategy. The White House. Available from: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[53] 2023-2030 Australian Cyber Security Strategy, Australian Government Office of Home Affairs; 2023-203 Australian Cyber Security Strategy Action Plan. Available from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf, 2023-cyber-security-strategy-action-plan.pdf (homeaffairs.gov.au)

[54] Cabinet Office. National Cyber Strategy 2022. 2022. https://www.gov.uk/government/publications/national-cyber-strategy-2022

[55] O'Rourke R. Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress. Congressional Research Service, R45757. Available from:https://www.crsreports.congress.gov/product/details?prodcode=R45757

[56] Gould J, Harris B. Big AUKUS news coming, but Hill and allies see tech sharing snags. Defense News. 2023. Available from: https://www.defensenews.com/pentagon/2023/03/07/big-aukus-news-coming-but-hill-and-allies-seetech-sharing-snags/

[57] UK Royal Navy Acquires Latest Generation REMUS 100s. Brooke-Holland L. AUKUS Pillar 2: Advanced Capabilities Programmes. HII Press Release. 2022. Available from: https://www.hii.com/news/united-kingdom-royal-navy-acquires-remus-100-unmanned-underwater-vehicle/

[58] Rahmat R. Indo Pacific 2022: Royal Australian Navy breaks cover on Speartooth large unmanned underwater vehicle. Janes. 2022. Available from: https://www.janes.com/defence-news/news-detail/indo-pacific-2022-royal-australian-navybreaks-cover-on-speartooth-large-unmanned-underwater-vehicle

[59] U.S. Department of Defense. FACTSHEET: Implementation of the Australia-United Kingdom-United States Partnership (AUKUS). 2022. Available from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/

[60] Department of Defense FY 2024 Budget Estimates. Defense-Wide RDT&E Justification Book Volume 3 of 5. Office of the Secretary of Defense. 2023. Available from: https://www.comptroller.defense.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/03_RDT_and_E/OSD_PB2024.pdf

[61] Ghost Shark a Stealthy 'Game-Changer'. Australian Department of Defence. 2022. Available from: https://www.defence.gov.au/news-events/news/2022-12-14/ghost-shark-stealthy-game-changer

[62] Australian Government: Defence. Uncrewed Undersea Capabilities Strengthen AUKUS Partnership. 2023. Available from: https://www.defence.gov.au/news-events/releases/2023-11-10/uncrewed-undersea-capabilities-strengthen-aukus-partnership

[63] Kumar R. Securing the Digital Seabed: Countering China's Underwater Ambitions. Journal of Indo-Pacific Affairs. 2023. Available from: https://www.airuniversity.af.edu/JIPA/Display/Article/3588497/securing-the-digital-seabed-countering-chinas-underwater-ambitions/

[64] Honrada G. US yielding its submarine warfare edge over China. Asia Times. 2023. Available from: https://www.asiatimes.com/2023/11/us-yielding-its-submarine-warfare-edge-over-china/

[65] AUKUS Fact Sheet. The White House. 2022. Available from: https://www.whitehouse.gov/briefing-room/statementsreleases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/

[66] Katz J. AUKUS nations take aim at robotic ground vehicles under threat of electronic warfare. Breaking Defense. 2024. Available from: https://www.breakingdefense.com/2024/02/aukus-nations-take-aim-at-ground-vehicles-under-threat-of-electronic-warfare/

[67] Gill J. Here are the Army's new planned EW, signals programs. Breaking Defense. 2023. Available from: https://breakingdefense.com/2023/12/here-are-the-armys-new-planned-ew-signals-programs/

[68] E-7A AEW&C. Boeing. Available from: https://www.boeing.com/defense/e-7-airborne-early-warning-and-control/

[69] U.S. Department of Defense. AUKUS Defense Scientists Test Robotic Vehicles. Department of Defense. 2024. Available from: https://www.defense.gov/News/Releases/Release/Article/3666171/aukus-defense-scientists-test-robotic-vehicles/

[70] Seldin J. China establishing 'commanding lead' with key military technologies. Voice of America. 2023. Available from: https://www.voanews.com/a/china-establishing-commanding-lead-with-key-military-technologies-/7124026.html

[71] Lewis J. AUKUS: A Generational Opportunity: Testimony. Washington, D.C: U.S. Senate Foreign Relations Committee; 2023. Available from: https://www.state.gov/aukus-a-generational-opportunity/

[72] Scarlett K, Lee D, Lubin A, Perlin P. Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us About Intelligence-Sharing Agreements. Yale Law School. 2018. Available from: https://www.law.yale.edu/mfia/case-disclosed/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing

[73] U.S. Embassy & Consulates in Australia. AUKUS Joint Leaders' Statement. 2023. Available from: https://www.au.usembassy.gov/aukus-joint-leaders-statement/

[74] Martin T. Australia developing 'top secret' intelligence cloud to work with US, UK spy agencies. Breaking Defense: Indo-Pacific. 2023. Available from: https://www.breakingdefense.com/2023/12/australia-developing-top-secret-intelligence-cloud-to-share-with-us-uk-spy-agencies/

[75] U.S. Department of Defense. AUKUS Defense Ministers Meeting Joint Statement. Department of Defense. 2023. Available from: https://www.defense.gov/News/Releases/Release/Article/3604511/aukus-defense-ministers-meeting-joint-statement/

[76] Moroney JD, Tidwell P. Making AUKUS Work. RAND. 2022. Available from: https://www.rand.org/blog/2022/03/making-aukus-work.htm

[77] Greenwalt W. Should New Zealand join in a five eyes defense industrial base? American Enterprise Institute. 2022. Available from: https://www.aei.org/foreign-and-defense-policy/should-new-zealand-join-in-a-five-eyes-defense-industrial-base/

[78] Oswald, R. Lawmakers Seek to Ease Defense Export Controls to UK, Australia. Roll Call, May

23, 2023. Available from: https://www.rollcall.com/2023/05/23/lawmakers-seek-to-ease-defense-export-controls-to-uk-australia/ Shah

[79] U.S. Export Rules Need Major Reform if AUKUS is to Succeed. Australian Strategic Policy Institute: The Strategist. 2023. Available from: https://www.aspistrategist.org.au/us-export-rules-needmajor-reform-if-aukus-is-to-succeed

[80] Reuters. More Work Needed on AUKUS Technology Sharing—British, Australian Officials. Reuters. 2023. Available from: https://www.reuters.com/world/more-work-needed-aukus-technology-sharing-british-australian-officials-2023-03-01/

[81] Horowitz MC, Pindyck. What is a military innovation and why it matters. Journal of Strategic Studies. 2023;**46**(1)

[82] Nemeth B. Military Innovation and Capability Development in a Multinational Context: The Costs and Benefits of Multinational Cooperation. Air Power Journal. 2022. Available from: https://www.diacc.ae/resources/2022_Bence_Nemeth_Military_Innovation_Capability_Development_Multinational_Context.pdf

[83] Varrall M. AUKUS: What are the Implications for Australia and the Region? KPMG. 2021. Available from: https://www.kpmg.com/au/en/home/insights/2021/09/aukus-implications-for-austaralia-and-the-region.html

[84] Jackett J. Defence Innovation and the Australian National Interest. Defence and Security Institute. University of Western Australia; 2023. Available from: https://www.defenceuwa.com.au/wp-content/uploads/2023/06/Black-Swan-Strategy-Paper-Issue09_Defence-Innovation.pdf

[85] Picucci PM, Angevine R, Roberts M, Sparrow D. Categorizing defense innovation. Defense Acquisition Magazine. 2021. Available from: https://www.dau.edu/library/defense-atl/blog/Categorizing-Defense-Innovation

[86] Katz JA. AUKUS partners announce pillar II plans: Maritime exercises, DIU challenges, industry forums. Breaking Defense: Indo-Pacific. 2023. Available from: https://www.breakingdefense.com/2023/12/austin-aukus-partners-announce-pillar-ii-plans-maritime-exercises-diu-challenges-industry-forums/

[87] Gallagher, M. DOD must move faster to leverage commercial technology. Real Clear Defense. 2022. Available from: https://www.realcleardefense.com/articles/2022/09/10/dod_must_move_faster_to_leverage_commercial_technology_852836.html

[88] McGinn JG, Roche MT. Developing a 'build allied' approach to increasing industrial base capacity. Naval Postgraduate School Acquisition Research Program. 2023. Available from: https://www.dair.nps.edu/bitstream/123456789/4835/1/SYM-AM-23-067.pdf

[89] Gaida J, Wong-Leung J, Robin S, Cave D. ASPI's critical technology tracker: AUKUS Updates. Australian Strategic Policy Institute. 2023. Available from: https://www.aspi.org.au/report/critical-technology-tracker

[90] Yaacob AR. AUKUS brings more than nuclear submarines to southeast Asia. East Asia Forum. 2023. Available from: https://www.eastasiaforum.org/2023/09/15/aukus-brings-more-than-nuclear-submarines-to-southeast-asia/

[91] Artificial intelligence: DOD should improve strategies, inventory process, and collaboration guidance. Government Accountability Office. 2022. Available from: https://www.gao.gov/assets/gao-22-105834.pdf

[92] Corben T. AUKUS: A year on—What to make of AUKUS after 365 days? Royal United Services Institute of New South Wales. 2022. Available from: https://www.rusinsw.org.au/Papers/20221123B.pdf

[93] Charlton GC, Gao X. Canada and New Zealand need to consider joining pillar 2 of AUKUS. The Diplomat. 2023. Available from: https://www.thediplomat.com/2023/09/canada-and-new-zealand-need-to-consider-joining-pillar-2-of-aukus/

[94] Clark C. With Australia, New Zealand to explore AUKUS 'opportunities'. Breaking Defense. 2024. Available from: https://www.breakingdefense.com/2024/02/with-australia-new-zealand-to-explore-aukus-opportunities-closer-to-joining/

[95] New Zealand may Join AUKUS Pact's Non-Nuclear Component. The Guardian. 2023. Available from: https://www.theguardian.com/world/2023/mar/28/new-zealand-may-join-aukus-pacts-non-nuclear-component

[96] Steff R. AUKUS + NZ=Win-Win. The Lowy Institute. 2023. Available from: https://www.lowyinstitute.org/the-interpreter/aukus-nz-win-win

[97] Fife R, Chase S. Canada seeks to join non-nuclear pillar of AUKUS alliance. The Globe and Mail. 2023. Available from: https://www.theglobeandmail.com/politics/article-canada-eyes-entry-into-aukus-alliance-to-helpkeep-china-in-check/

[98] Hernandez-Roy C. Canadian membership in AUKUS: A time for action. Center for Strategic and International Studies; 2023. Available from: https://www.csis.org/analysis/canadian-membershipaukus-time-action

[99] Bell CL. Australia should support japan and South Korea's accession into AUKUS. The Diplomat. 2023. Available from: https://www.thediplomat.com/2023/10/australia-should-support-japan-and-south-koreas-accession-into-aukus/

Chapter 8

Perspective Chapter: Post Offices and National Security during War

Hussain Syed Gowhor

Abstract

National security in the digital and information age may be jeopardized if a war breaks out internationally. At first, enemy countries may conduct air raids and hacking operations to destabilize and destroy all the electronic media of communication through bombardment and cyberattacks. In that case, a government must have a backup physical medium of communication to maintain not only communication within the government but also civilian communication. During this era of modern information and communication technology, the roles of post offices are redefined in the light of their roles during past wars in terms of building a more resilient society during modern warfare, which requires an assessment of the current level of readiness, adaptability and flexibility of the military to run the postal organization during war. Last but not the least, the article provides different case studies of postal operations during different wars. This article will refresh the knowledge of postal operations during wartime among postal as well as military officials.

Keywords: national security, war, physical and electronic medium of communication, national resilience, base and field post offices, ontological security

1. Introduction

Have you ever thought of a world where the electronic communication system has broken down completely due to the onset of an international war? How would individuals and organizations communicate with their counterparts in that situation? In this age of modern technologies, many people often underrate the role and contribution of post offices in communication. Most of the people often argue that email has made the role of post offices blurred and has diminished its utility in today's society. However, these people often overlook the role of post offices in maintaining the sovereignty of a state. Have these people ever thought of the fact that national security in the digital and information age may be jeopardized if a war breaks out internationally? Air strikes are usually the first activity during the war, which is used to destroy all the electronic mediums of communication of an enemy country through bombardment [1]. Moreover, there are chances of cyber warfare, where cyberattacks can render all the online systems dysfunctional. In that case, a government must have a backup physical medium of communication to maintain not only communication within the government but also civilian communication. That is why even during this age of technology, the government still retains the control over post offices despite its being a losing concern for the government.

A nation should maintain a degree of resilience in order to revert to the physical medium of communication during war. During this era of modern information and communication technology, the role of post offices can be redefined in the light of their roles during past wars in terms of building a more resilient society during modern warfare. This article will refresh the knowledge of postal operations during wartime among postal as well as military personnel.

2. Methodology

The aim of the chapter is to inform the readers about the potential role of post offices in maintaining national security during war. In doing so, this chapter uses several methodologies. First of all, it reviews the existing literature in the field of war and national resilience to understand what roles are expected from post offices during wars. Secondly, it uses historical narratives to demonstrate how postal operations were conducted during war and how post offices contributed to maintaining national security during past wars. The exploration of some selected historical case studies is aimed at showing possible uses or means for post offices to be utilized to overcome the loss of infrastructure from attacks in wartime, which would work as possible lessons for the future wars. The use of historical narratives of the past wars has limitations in the sense that modern warfare is most likely to be drastically different from the past wars in respect of types of attacks, types of targets, means of attack and so on. Thirdly, based on the past case studies on different wars, the potential roles of post offices for modern war were derived as a possible solution to the problem of loss of electronic infrastructure during war. These roles are not meant to be specific to a certain country or for a certain point of time in history. Rather, they are to be deemed as an ideal solution to the problem rather than a universal approach. The relationship between modern potential roles and national security was analyzed and evaluated in the light of the existing literature in the field of security studies. Fourthly, readiness, adaptability and flexibility of the Army of different states in running postal organizations were assessed because it is recommended that the postal department come under the general command of the Army during the war and postal operations need to be conducted manually during the war because of the destruction of technologies. To conduct such assessment, a measure of correlation was used to find the association between ranks of military strengths and postal resilience score for 132 countries of the world. Lastly, literature on modern war and resilience was reviewed to explore the relevance of post offices in respect of national security.

3. Literature review

Any discourse on war remains incomplete without referring to some of its fundamental literature. As such, this section attempts to relate post offices' role in national security during the war by referring it to the work of Carl von Clausewitz and other prominent authors on modern war and national resilience. This section will inform the readers about the roles that are expected from post offices during wars.

3.1 Clausewitz

A sensible starting point in this regard should be the "remarkable trinity" in war introduced by Clausewitz, which is used as "a central analytical framework for

comprehending the nature of war" [2]. Clausewitz's trinity is composed of the people, the commander and his Army and the government [3] that try to capture the "human elements of war, the interactive dynamics of war and the centrality of fighting" [4]. In this trinity, the post office obviously falls within the last element of the trinity, that is, the government because the post office usually exists as a government department. During war, a government introduces "the rational calculus of war in order to protect the interest of the state, provide the goals for war, maximize and preserve the strength of the state relative to other states, and devise the overall strategic direction, including the matching of resources and expenditures to anticipated gains" [3]. Post offices play a vital role in this rational calculus by maximizing and preserving the strength of the state relative to other states in respect of communication. During war, a robust physical medium of communication can be a differentiating factor for success among states. Post offices have also a role to play in respect of mobilizing various types of resources on behalf of the government during war.

In his book one, chapter six, Clausewitz dwelled over intelligence in war, which has much to do with the post office. Intelligence is defined as every sort of information about the enemy and its country. The term "communication" is inextricably linked with the term "information." At present, there are "varied means of communication" that "revolutionized the ability of commanders to receive information from and on the battlefield, allowing them to dispatch their orders and decisions much more effectively than in Napoleon's time [3]. Handel [3] argues that Clausewitz' (and even more so Tolstoy's) pessimistic view of the commanders' lack of effective control over the course of events on the battlefield is no longer justified—certainly not from the technical point of view because the difficulties in receiving and transmitting information on the battlefield have been reduced considerably. However, this is not true because during modern warfare, the technological equipment is not expected to be in order because of their dependence on transmission towers, which will be destroyed by air raids. In that case, post offices come as the savior for the commanders to receive and dispatch information and orders from and to the field staff.

Clausewitz has mentioned about the "sense of locality" as an important attribute of the commanders [4]. When an Army moves to a new locality, whose geography and people are completely unknown to them, they must rely on local guides and spies to provide them information on the local geography and people. Post office people are well versed in these two things by virtue of their nature of work. As such, they are the most suitable people to help Armies become conversant with local conditions.

Clausewitz was also concerned about the geographical dimension of war [4]. The most striking aspect of the geographical dimensions of war is the geographical limitation. McInnes [5] notes how, during the nineteenth and twentieth centuries, "Geographical limitations were overcome by improvements in transportation, enabling armies of hundreds of thousands to be moved and supplied over large distances." The postal sector's capacity in respect of logistics and delivery undoubtedly helps in overcoming the geographical limitations during war.

3.2 Creveld

Creveld emphasizes on the military balance as a *sine qua non* for winning a war [6]. He points out that military balance depends on the effective use of a multimodal communication system during war. He provides accounts of some records of failures during war, where some failures were due to interrupted communication. He underscores the supportive role of the non-combatants, which include civilian organizations

including post offices during war. Finally, he discussed about the obstacles to force, where communication obstacles are very crucial.

3.3 Tuck

Tuck delineates the principles of land warfare, where he emphasizes on the coordination between the Army and other state agencies as a precondition for success in land warfare [7]. He particularly mentioned the role of stable and uninterrupted communication infrastructure during war. Post offices, as a physical medium of communication and a state agency, thus contribute towards the success of military in war.

3.4 Simpson

Simpson pointed out that war consists of a fragmented and polarized dynamics implying that war affects every infrastructure and institution in a country [8]. Thus, the post office is not an exception during war. Simpson emphasizes the traditional use of armed force to seek to create military conditions within which a political settlement can be reached. However, creating such a conducive military condition hinges on the support of other organizations in a state, including the post office.

3.5 Lewin

Lewin shows through several case studies how resilience during war can save nations from the devastating consequences [9]. As part of national resilience, he proposed the deployment of a number of techniques that would render the effectiveness of resilience programs by matching together the different factors of national resilience. In his model, he shows different combinations of factors and the resultant effects on national resilience. The combination of military and postal sectors has a distinct place in his model that leads toward improved national resilience in the communication sector of a country.

4. Postal operation during war

It may be mentioned that, during a war, a state's backbone communication infrastructure is destroyed partially or thoroughly. As a result, the state of physical medium of communication gets back to a primitive state, where little or no technology is used to perform postal operations, that is, mail collection, transmission and delivery. Rather, every operation is performed manually. In that case, one can assume that the postal services would be conducted in a manner similar to that during the Second World War. As such, it would be the most appropriate to describe how postal operations are carried out during war in the light of the situation that prevailed during the Second World War. The Postal War Manual which was published in 1937 provides a fairly accurate description in this regard [10]. As such, the next paragraphs in this section have been taken from that book with a view to provide the readers with a comprehensive understanding of how postal operations are conducted during war.

During war, the postal service should come under the general command of the Army. The postal officials wear the ranks and badges of military personnel. During war, the units formed by the postal services on mobilization are termed as base postal depot, base post offices and field post offices. The Base postal depot works as a postal

clearing house, inquiry bureau, forwarding office and returned letter office for all field units. It also acts as the record office and depot for postal units and deals with the postal stock depots regarding issues of technical equipment. There are separate rules regarding the war establishments of field postal units.

The location of the base postal depot is decided by the head of the postal department in consultation with the Army Headquarters. Vicinity of the cantonments, field offices of the Armies, mail communication system and war situation at a certain locality, to name a very few, are some of the determining factors in this regard. One or more base post offices are opened as the channel of communication between the state and the field, and *vice versa*. Ordinarily, a base post office is established at each important military base of operations. In the case of overseas expeditions, base post offices are preferably established at the main post of disembarkation. A base post office works as the head post office and a field post office works as the sub-post office in account with the base post office.

The postal services of an Army or force in the field are controlled by the officers of the postal service. These officers are attached to the general headquarters and the headquarters of the Armies. They receive the orders of their commanders through "Q" staff of the headquarters concerned. These officers are senior officials of the postal department who are equivalent to the position of Postmaster Generals.

The Director General of the Postal Department will issue instructions for mobilization of all postal units included in the mobilization plan. During the course of operation, the Director of Postal Services will advise the Force Commander with regard to postal services. In the event of additional units required, the Force Commander will apply to the Quarter Master General, who will inform the Director General of the Postal Department of the requirements. The Director General will then issue orders for the raising of additional units. In the case of operations not entailing mobilization, the command concerned may arrange direct with the Postmaster General of the postal circle for the provision of such field post office and base post offices as the circumstances require after obtaining approval from the Army Headquarters. The Quarter Master General will keep the Director General of Postal Department of such arrangements. Field post offices will be established on the lines of communication as required. The Director of Postal Service or his authorized representative will take a decision in this regard in consultation with the Army and Postal Headquarters.

On general mobilization, all supervising postal officers selected for field service will be granted commissions in the Army in reserve core and will be given temporary military rank and other amenities entitled to a military officer of equivalent pay or grade. Other subordinate staffs will also be entitled to rank as equivalent to their corresponding pay or grade. The postal officers and staffs mobilized for field service will be controlled by the Army Act. They will have to observe necessary practices relating to secrecy and confidentiality. Relating to departmental offenses, the officers and staffs of post offices will be disciplined departmentally. Military and civil offenses will be dealt with by military authorities under the orders of the commander of the formation or unit to which the offender may be attached, and any sentence awarded by them, either summarily or by order of a court-martial, will be carried out by the military authorities. Unless someone commits a felony, he or she will be kept in his or her duties in the condition of open arrest and will be trialed under the departmental laws and not by the military act. Postal officers who have been granted commissions will wear uniforms and badges of rank. Subordinates will be supplied with field service clothing and kits. Non-combatants will receive the prescribed uniform. All postal officers and staffs will wear brass shoulder titles inscribed "Post." Those who are not supplied with uniform will wear identity discs or cards, which will have the words "Post Office" and a consecutive number stamped

thereon. There will be a separate war establishment manual that will govern the matters relating to establishments of postal officers and staffs during war.

Postal officers who will be commissioned will be armed like an officer of an infantry battalion of equivalent rank. There will be separate war equipment manual that will contain details of mobilization equipment. The equipment of postal units, both military and technical, is kept in peace by the headquarters of formations to which the concerned postal units will be attached on mobilization. It will be issued to postal personnel when they join their respective headquarters on mobilization. Field post offices will fly a distinguishing flag by day and by night and will show the distinguishing lamps as will be supplied to them as per the war equipment manual. Subsequent to mobilization, supplies of military equipment will be obtained by postal units from the nearest ordnance depot. Supplies of technical equipment will be obtained by the field post offices from the base post offices, which will indent upon the base postal depot. All the postal officers and staffs will be responsible for safekeeping of the equipment. It must be handed over under receipt from one officer to another officer when relieving from duties in the case of transfer. On completion of a campaign, postal units will hand in military equipment (of ordnance issue) to the headquarters of the formations to which they will be attached during the campaign. All technical equipment (of postal issue) will be handed into the base postal depot. The base postal depot on receipt of the technical equipment from the postal units in the presence of the official in charge of the unit will complete the equipment of each particular unit to scale and transfer it to the headquarters of the respective formations to which they will be attached on mobilization.

In order to run the postal service smoothly during war, a post is created called Director of Postal Service, who is assisted by the Assistant Director of Postal Service and Deputy Assistant Director of Postal Service. These assistants are posted at the field and base post offices. The Director of Postal Service exercises the power of a Postmaster General. He or she will usually be at the general headquarters of the Army but will be moving frequently to visit the base and field post offices. He or she will also act as the advisor to the military authorities on all postal matters. The orders of the Force Commander will be conveyed to him or her through "Q" staffs. He or she will be responsible for proper arrangements and posting of subordinate staffs to various field and base post offices. Post offices are required to prepare and submit daily as well as annual reports of their activities to the higher authorities.

The Director of Postal Service and the Assistant Directors of Postal Service will arrange with Army for Force Headquarters for the carriage of the mails between base and field post offices. The Quartermaster General will arrange for the transport and all other logistics support for carrying mails. Detailed instructions will be issued regarding the manner of dispatching mails. Financial services rendered by post offices will continue as long as there is a smooth provision of disposing excess cash on a daily basis. All important questions affecting postal arrangements will be settled by the Director of Postal Service under the orders of the Force Commander. However, in case of minute details and also in the case of urgency, senior local postal officials may take action with the concurrence of the nearest military authority.

5. Case studies on post offices and its role in war

During past wars, the role of postal officials was undeniable in maintaining nationwide communications. Following are some case studies that help us to assimilate the role of post offices during war.

5.1 World war I

As can be found from a BBC report, delivering 12 million letters a week and the commitment of the postal staffs to deliver the replied letters back to the UK is a clear sign of the efficiency of postal service during World War I [11]. As can be learnt from Ref. [12], during World War I in the UK, "post office had its own regiment called 'The Post Office Rifles' to fight on the frontline. Carrier pigeons were used to deliver post during that war." As can be found in Frank's diary [13], during World War I, "all mail destined for the armed forces was routed through the Home Postal Depot in London for sorting and despatch. The primary depot was a huge, wooden, purpose-built structure set on five acres of Regent's Park. Once processed, the mail was then sent on to Base Army Post Offices (BAPO) that existed in every theatre of war. From there, it was distributed to the Field Post Offices, mobile units that were close to the front. Unit Postal Orderlies collected the mail from there and delivered it to the troops. The Army Postal Service ran the Base Army and Field Post Offices. By the end of the war, it had over 7,000 men and women serving in it, all of whom were seconded from the General Post Office. The service worked very well. A special correspondent for The Times reported on December 22nd 1917 that parcels arriving at the BAPO in France on the 18th had left Belfast on 13th and Glasgow on 14th and that letters were taking less than 48 hours from Aberdeen and Wolverhampton" [13].

5.2 World war II

"In 1939 the Postmaster General of the UK informed Postmasters across the country to allow parcels containing babies' Air Raid Precautions helmets to be carried via the inland parcel post, even if they exceeded the usual maximum dimensions" [14]. Duffield [14] adds that "the Post Office deployed Air Raid Precautions (A. R. P.) to protect their buildings, which had great importance to both civilians and the military in maintaining postal and telephone communications." Crowley [15] highlights the role of post offices during the Second World War in the UK, which include changing the postal habits of the people, maintaining national morale and remaining post offices open even after the sounding of a public warning siren, to name a very few.

5.3 The liberation war of Bangladesh

The war was 9 months long that began on March 26, 1971, and ended on December 16, 1971. During the war, the first field post office was established in Mujibnagar, the temporary capital of the country. Besides, a set of eight postage stamps was published to mark the sovereignty of the country. It was mostly like a guerilla warfare and the postal people assisted the freedom fighters by carrying arms and ammunitions inside postal bags. They also provided secret information about the Pakistan occupation forces, particularly their positions, bunkers, etc. [16].

5.4 Ukraine war

Ukraine War with Russia is the latest example of how post offices help in maintaining national security during war. As can be found in the report of AlJazeera [17], banks have closed in Ukraine and *post offices are stepping up to provide financial services while also delivering mail and humanitarian aid. The department reiterates its*

firm determination to remain open amid all adversities. For example, the department has opened mobile post offices as more than 500 post offices have been destroyed. It has also published commemorative stamps to boost up the morale of the Ukrainian people.

6. Modern potential roles

Taking lessons from the above wars, it can be deduced that, during a modern warfare, post offices have the scope to assume the following roles as a possible solution to the loss of electronic infrastructure during war that may render it as a front organization in upholding and maintaining national security of a state during war.

6.1 Keeping communication uninterrupted

Keeping the physical communications uninterrupted during a war is a major challenge for post offices. As can be learnt from the previous sections, during the World Wars, postal services remained uninterrupted amid many obstacles. Even during the modern war, such as the ones going on in Ukraine and Palestine, the postal services are running smoothly without major disruptions. As the physical infrastructure, such as roads and bridges are destroyed, the mail communications are disrupted. Nevertheless, the post office people have always shown their firm commitment to keep mail communication uninterrupted. There is a saying in the post offices that "mail must move (mmm)" under any circumstances. Post offices usually deploy a relay system of mail communication, where a runner travels a certain distance and hands over the mail bags to another runner to travel further toward destination.

6.2 Security of the lives of the common people

During war, people cannot come to post offices and even cannot go elsewhere to fulfill their quotidian necessities because if they go outside, their life will be jeopardized. The post office comes at the forefront in this situation. Post office staffs go to the doorstep of the common people to collect and deliver mails that contain essential commodities required for living their day-to-day life.

6.3 Postal force mobilization

Postal force mobilization refers to the process of transferring the postal officers and staffs to the military establishment with a view to absorb them within the Army during war. Postal force mobilization involves tasks such as preparing the list of fit and willing officers and staffs, providing them with necessary training and so on. Detailed rules of mobilization are laid down in the Postal War Manual [10].

6.4 Formation of postal battalions

In addition to providing ancillary services, post office people also take part actively in war. For example, during World War II, the Local Defense Volunteers in the UK were trained to operate anti-aircraft weapons, grenades, and to fight with bayonets. The post office forms their own battalions during war. For instance, Post Office Rifle Clubs were formed during World War I [12].

6.5 Safekeeping of government exchequer

A considerable amount of cash, stamps and other valuables that form the part of government treasury is stored in the post office vaults. Post office people assume it as their solemn duty to ensure security of those cash, stamps and other valuables. Post office people are always ready to dedicate their lives for the sake of ensuring security of these cash, stamps and valuables under their custody. For example, during the liberation war of Bangladesh in 1971, the Senior Postmaster of Chottogram (formerly Chittagong) GPO refused to hand over the key of the treasury vault room to the occupational forces of the Pakistan Army [16].

6.6 Safekeeping of customer information

War can be of various types. The war I have discussed so far is about the political war that concerns the sovereignty of a country. Another type of war is economic war which concerns the autarky and economic well-being of the country and its citizens. Even another type of war is information warfare which concerns the privacy of information of customers. The latter two types of war have devastating consequences on the economic lives of the citizens of a country. Post offices work for the safekeeping of customers' information relating to their address database and consumer's purchase behavior during economic and information warfare. For example, if the consumers' purchase behavior and their address database that are preserved by post offices are leaked, it will suffice to ruin the backbone of an economy in a number of ways, such as through supplying credit card information to the hackers of enemy countries and supplying purchase behavior information to the agents of product manufacturers of enemy countries.

6.7 Carrying and delivering military supplies

Although military convoys are deployed during war for carrying military supplies, there may be some technical, tactical and diplomatic issues that may entail use of postal service for carrying and delivering military supplies. For example, a postal supply chain may be used to send the supplies in a disguised way. During the liberation war of Bangladesh which was one type of guerilla warfare, the postal runners and mail carriers used to carry the arms and ammunitions on behalf of the freedom fighters. Besides, when an Army camp is situated at a distant place where military vehicles cannot go, postal runners may be used for delivering military supplies in small quantities.

6.8 Intercepting and checking articles

The main purpose is to detect if any mail contains any written matter, such as a propaganda, a cipher message and so on, which are subversive to the state security. A prime concern is to detect if a letter or parcel contains any dangerous article that may be a serious threat to national security. There may be chemical, biological, radiological and nuclear (CBRN) weapons inside a parcel. For example, there was an anthrax attack by mail in 2001 [18]. So, it is very usual that enemies will try to use the postal service to spread CBRN weapons during war. A related concept in this regard is field censorship. Instructions regarding field censorship that is the censorship of correspondences addressed to or emanating from persons in a theater of operations will

be issued to all concerned when the decision to impose field censorship is imposed. Efficient field censorship depends greatly on close co-operation between the postal services and the field censorship staffs. If a field censorship is imposed, a censor officer along with supporting staffs will be appointed to each Army in the field. The postal staffs are required to hand over all the incoming and outgoing mails to the censor staffs for inspection [10].

6.9 Domestic surveillance

This role of post office has been identified by Conolly-Smith [19]. Postmen and runners work as the sources or informers for the armed forces to identify collaborators and traitors. Postmen visit door-to-door and have a good knowledge about the geography of the locality and the people residing there. They know better than the Army which are the best places to hide and which are the best places to launch an attack. They know the exit path of the locality. Thus, they help an Army to plan for an attack and to carry out reconnaissance. For example, during the liberation war of Bangladesh, the postal people such as postmen were of great help to the freedom fighters in this respect [16].

6.10 Backup of online systems

Another form of warfare is cyber war, where cyberattacks are common to debilitate the online systems. In that case, the post offices work as a backup of those systems. For instance, if the financial services, such as Automated Teller Machine (ATM), Electronic Fund Transfer (EFT), Mobile Financial Services (MFS) and other online remittance systems collapse during war due to cyberattacks or physical damage, then the post offices' traditional money order system will be the server of the last resort.

6.11 Philatelic matters relating to sovereignty

This is particularly common when a nation is engaged in a liberation war to free itself from foreign occupation forces. Bangladesh is a burning example in this regard. In 1971, immediately after declaration of the independence and formation of the government in exile, the government of Bangladesh took initiative to publish the first postage stamp as a token of its sovereignty and independence. This stamp played a vital role in gaining recognition from other states [20].

7. What these roles have to do with national security?

By playing the above roles, post offices ensure national security during war through ontological security. Zarakol [21] argues that ontological security is more important than the sovereignty of a state. Zarakol further argues that ontological security is contrary to the idea that state is "a unitary actor" [21], and thus, it follows that in order to ensure ontological security, the states must think of themselves as part of the global system and thus the states must think beyond the concept of national sovereignty in order to ensure ontological security. Post offices consider the world as a single postal territory [22]. No war can stop the movement of mails across the border. Even if a mail bag is received from an enemy state as a transit to forward it to a third

state, the state receiving the mail has no right to detain it. For example, we can know from the report of AlJazeera [17] that the Universal Postal Union helped to reconstruct postal infrastructure and restore Ukrainian postal services. It took a number of steps to support Ukraine, such as waiving charges for the delivery of postal items to Ukraine, distributing large amounts of goods and raising funds. The result was that international postal exchanges remained unhindered by Russian military actions.

National security is a matter of concerted efforts of all the players in a state. Although the armed forces play the first fiddle about the national security during war, it cannot ensure national security without the help of other agencies of the government. It should be remembered that not all department's role becomes active and visible during war at all times. Rather, it depends on situations. Some situations may arise during war that can render the postal department as more important than any other department that provides support to the armed forces. For example, when wireless apparatuses cease to operate due to a lack of signals in remote and hard-to-reach areas, the post offices will come as the savior for the armed forces to reach urgent messages to the Army camps in those areas. It is the post office staffs who are more aware than any other staffs in other government departments about the physical communication system in a locality. Thus, their services become essential for both communication, espionage and reconnaissance purposes.

8. An assessment of the readiness, adaptability and flexibility of military of different states to run the postal organization during war

If a war breaks out internationally, the first and foremost attack will be undoubtedly on the electronic media of communication and its infrastructure. It is expected that they will be destroyed completely and will not be operational until the end of war. In that case, people will have to change their postal habits, and the whole postal system will go back to the primitive state, where people will maintain communication through a physical medium, that is, post office and mails will be collected, transmitted and delivered manually. The most striking change will be that the whole postal organization will come under the military command and control. If this happens, it entails an assessment of the readiness, adaptability and flexibility of the military to run the postal organization during war. At present, there is no recognized measure or index to determine such readiness, adaptability and flexibility. The Global Firepower is an index that ranks military strengths of different states of the world. This ranking utilizes sixty individual factors to determine the power index. However, none of these factors measure the readiness, adaptability and flexibility of the military forces of the world [23]. As such, we need to use another alternative method to assess the readiness, adaptability and flexibility of the military of different states to run the postal organization during war. It is interesting to note that the Universal Postal Union publishes a Postal Development Report that contains a score of various countries relating to postal resilience [24]. To me, it makes sense to calculate the rank correlation coefficient through Spearman's ρ as the measure of association between the rank of military strengths and postal resilience score for 132 countries of the world (provided in Appendix-1) in order to determine the strength of relationship between these two ranks. As the Global Firepower index does not have any such index to measure the readiness, adaptability and flexibility, the rank correlation coefficient between the ranks of military strengths and postal resilience score for 132 countries of the world may provide a rough idea about the state of readiness, adaptability and flexibility of

the military of different states to run the postal organization during war. The formula used for computing Spearman's ρ is as follows [25–27]:

$$\rho = 1 - \frac{6\Sigma d^2}{n\left(n^2 - 1\right)} \tag{1}$$

where

d = the difference between each rank of corresponding values of independent and dependent variables

n = the number of pairs of values

The value of Spearman's ρ was 0.35, which indicates a moderately positive correlation between ranks of military strengths and postal resilience score for 132 countries of the world. It implies that the military forces of the world are moderately resilient to embrace the postal system during war.

To assess the readiness, adaptability and flexibility of the military of different states to run the postal organization during war, I have looked at the present state of relationship between the postal and the military departments. I have taken the United States of America (USA), the United Kingdom (UK) and Russia as the sample states to look at such relationships.

In the USA, there is a separate military postal service agency that processes military mail. The United States postal services explains military mail as follows:

> *"The Department of Defense is a key partner in extending Postal Service products and services to the American Armed Forces overseas. The Postal Service uses its international distribution and transportation services to support the Department of Defense around the world. Overseas military mail is mail matter delivered to APOs (Army Post Offices for Army and Air Force personnel) and FPOs (Fleet Post Offices for Navy and Marine Corps personnel). This service is an extension of the domestic service and includes all mail addressed to or mailed from a military unit or between two military units overseas. The Postal Service is committed to providing top operational service to American service men and women stationed overseas" [28].*

Section 406 of Title 39 United States Code provides the legal authority for the Department of Defense (DoD) to establish branch post offices and enter into an agreement with USPS. So, DoD personnel are authorized to provide mail service to DoD patrons [29]. Under this rule, the armed forces can establish military post offices, that is, APOs and FPOs [29].

In the UK, a dedicated military postal unit, the Army Post Office Corps was formed in 1882. It was transformed into a new organization called British Forces Post Offices (BFPO) in 1990 [30].

As can be known from [31], Russia has a very good tradition of a systematic and well-organized postal service that has been prevalent since 1700 A.D. Moreover, as can be known from [31], Lenin, just after Russian revolution, vowed to organize "the whole national economy on the lines of the postal service." This implies that military service in Russia is also keen to accept the postal system. Thus, it can be argued that while in the UK and the USA, the military is shaping the postal operations because they have separate military mail service. In Russia, the postal service is shaping military operations because the military organizations had to follow the postal structure after the Russian revolution.

9. Conclusion

The extant literature in the fields of war and national resilience indirectly supports the roles of post offices in respect of national security during war. In the light of the lessons learnt from previous wars, it can be concluded that post offices proved itself as a reliable organization during the past wars in terms of providing uninterrupted communications services. However, the situations that may prevail during any modern war are expected to be remarkably different from those in the previous wars. Therefore, post offices are expected to play a more extensive role than in the past because it is apprehended that modern warfare may jeopardize the national security of a state through air attacks and cyberattacks, which will entail post offices to assume some roles conducive to national security, such as keeping communication uninterrupted, ensuring security of the lives of the common people, mobilizing postal force, forming postal battalions, safekeeping of government exchequer, safekeeping of customer information, carrying and delivering military supplies, intercepting and checking articles, ensuring domestic surveillance, acting as the backup of online systems and publishing philatelic matters relating to sovereignty, to name a few. As it is highly likely that postal organizations may become under the general command of the Army during war and that the postal service may have to return to a primitive state due to the destruction of communication technologies, there is an issue of national resilience during war, which entails the assessment of the readiness, adaptability and flexibility of the Army of different states in running postal organizations. Using a measure of association for 132 countries of the world, it was found that the military forces of the world are moderately resilient to embrace the postal system during war.

As water has no constant form, there are no constant conditions in war [32]. War operates in a volatile environment that can entail the support of any organization crucial and vital during wartime. Although post offices can expect to be a vital and crucial player during war at any time, it should strive for making it more useful during war to the generals and statesmen. To this end, post offices must engage in new sorts of activities and services that would be useful during war. Apart from the functions discussed in this essay, some potential activities of post offices during war that may contribute toward enhancing national security may include conducting national security surveys, providing postal identities to the citizens and extending post restante services, to name a few. However, it is difficult to say which activities might emerge out of situational demand as the activities are crucial for maintaining national security. Thus, it would be wise for post offices to be ready all the time for taking up any role during war.

The most important thing for the post office is to convince the government that it has a glorious past in ensuring national security during war and it wishes to continue to contribute in the same way in the future. However, recent dwindling of the importance of its services has caused the loss of image and importance of the post office department and its people. Thus, in order to be considered as a vital player in ensuring national security, the first and foremost thing is to regain its social, economic, and political importance and its lost image through efficient operation of the existing services having value-added features and intrinsic appeal for the products and services it offers.

Appendix 1

See **Table A1**.

Sl.	Country	Military strength	Postal resilience score
1	Australia	16	24
2	Afghanistan	114	88
3	Albania	91	70
4	Algeria	26	86
5	Angola	55	102
6	Argentina	28	103
7	Armenia	94	39
8	Austria	84	5
9	Azerbaijan	57	85
10	Bahrain	79	79
11	Bangladesh	40	126
12	Belarus	60	1
13	Belgium	68	16
14	Belize	139	119
15	Benin	144	57
16	Bhutan	145	118
17	Bosnia and Herzegovina	133	4
18	Botswana	124	64
19	Brazil	12	21
20	Bulgaria	59	51
21	Burkina Faso	121	77
22	Cambodia	106	123
23	Cameroon	100	71
24	Canada	27	6
25	Central African Republic	136	132
26	Chad	97	120
27	Chile	46	41
28	China	3	40
29	Colombia	43	25
30	Congo	72	101
31	Congo (Rep.)	122	74
32	Croatia	69	50
33	Cuba	66	106
34	Czech Rep.	48	22
35	Denmark	50	125
36	Dominican Republic	118	62
37	Egypt	14	90
38	El Salvador	127	100

Sl.	Country	Military strength	Postal resilience score
39	Eritrea	113	112
40	Estonia	104	17
41	Ethiopia	49	75
42	Finland	51	96
43	France	9	7
44	Gabon	131	105
45	Georgia	85	44
46	Germany	25	27
47	Ghana	109	67
48	Great Britain	5	11
49	Greece	30	43
50	Guatemala	102	131
51	Honduras	92	130
52	Hungary	54	115
53	Iceland	137	52
54	India	4	58
55	Indonesia	13	36
56	Iran	17	35
57	Iraq	45	76
58	Ireland	90	8
59	Israel	18	20
60	Italy	10	9
61	Japan	8	31
62	Jordan	81	87
63	Kazakhstan	63	49
64	Kenya	87	59
65	Korea (Rep.)	6	47
66	Kuwait	78	129
67	Kyrgyzstan	107	28
68	Laos	115	83
69	Latvia	95	53
70	Lebanon	111	111
71	Liberia	141	99
72	Libya	80	94
73	Lithuania	93	23
74	Luxembourg	126	95
75	Madagascar	130	73
76	Malaysia	42	33

Sl.	Country	Military strength	Postal resilience score
77	Mali	110	108
78	Mauritania	132	42
79	Mexico	31	55
80	Moldova	143	34
81	Mongolia	99	92
82	Montenegro	128	56
83	Morocco	61	32
84	Mozambique	112	128
85	Myanmar	38	80
86	Nepal	129	110
87	Netherlands	39	15
88	New Zealand	103	19
89	Nicaragua	117	117
90	Niger	119	98
91	Nigeria	36	72
92	North Macedonia	108	65
93	Norway	35	45
94	Oman	76	114
95	Pakistan	7	93
96	Panama (Rep.)	135	107
97	Paraguay	88	89
98	Peru	53	82
99	Philippines	32	78
100	Poland	20	14
101	Portugal	41	12
102	Qatar	65	63
103	Romania	47	81
104	Russian Federation	2	10
105	Saudi Arabia	22	66
106	Senegal	125	97
107	Serbia	58	2
108	Sierra Leone	138	124
109	Singapore	29	13
110	Slovakia	67	18
111	Slovenia	86	46
112	South Africa	33	48
113	Spain	21	54
114	Sri Lanka	71	60
115	Sudan	75	38

Sl.	Country	Military strength	Postal resilience score
116	Suriname	140	127
117	Sweden	37	84
118	Switzerland	44	3
119	Tajikistan	120	116
120	Tanzania	101	69
121	Thailand	24	26
122	Tunisia	73	29
123	Turkey	11	37
124	Uganda	83	104
125	Ukraine	15	30
126	United Arab Emirates	56	122
127	United States of America	1	61
128	Uruguay	96	109
129	Uzbekistan	62	113
130	Vietnam	19	68
131	Zambia	89	121
132	Zimbabwe	98	91

Sources: (1) https://www.globalfirepower.com/countries-listing.php. (2) https://www.upu.int/UPU/media/upu/publications/postalDevelopmentReport2022.pdf.

Table A1.
Rank in military strength and postal resilience score for 132 countries of the world.

Author details

Hussain Syed Gowhor
Deputy Postmaster General and Instructor, Postal Academy, Bangladesh Post, Rajshahi, Bangladesh

*Address all correspondence to: gowhor@gmail.com

References

[1] Pape RA. Bombing to Win: Air Power and Coercion in War. London: Cornell University Press; 1996

[2] Waldman T. Continuity in Confusion: Understanding Clausewitz's Trinity [Internet]. 2013. Available from: https://www.researchgate.net/publication/331311814_Continuity_in_Confusion_Understanding_Clausewitz%27s_Trinity [Accessed: January 25, 2024]

[3] Handel MI. Clausewitz in the age of technology. Journal of Strategic Studies. 1986;**9**(2-3):51-92. DOI: 10.1080/01402398608437259

[4] Waldman T. War, Clausewitz, and the Trinity [Internet]. 2009. Available from: https://core.ac.uk/download/pdf/40048786.pdf [Accessed: January 25, 2024]

[5] McInnes C. Spectator-Sport Warfare: The West and Contemporary Conflict. Colorado: Lynne Rienner; 2002

[6] Van Creveld M. Transformation of War. London: The Free Press; 2009

[7] Jordan D, Kiras JD, Lonsdale DJ, Speller I, Tuck C, Walton CD. Understanding Modern Warfare. 1st ed. Cambridge: Cambridge University Press; 2008

[8] Simpson E. War from the Ground Up: Twenty-First-Century Combat as Politics. New York: Oxford University Press; 2013

[9] Lewin E. National Resilience during War: Refining the Decision-Making Model. New York: Lexington Books; 2012

[10] Ogilvie CMG. Postal Manual (War) India, 1937. New Delhi: Government of India; 1937

[11] BBC. World War One: How Did 12 Million Letters a Week Reach Soldiers? [Internet]. 2014. Available from: https://www.bbc.com/news/magazine-25934407 [Accessed: January 25, 2024]

[12] Trueman CN. The Role of the Post Office in World war one [Internet]. 2015. Available from: https://www.historylearningsite.co.uk/world-war-one/the-role-of-the-post-office-in-world-war-one/ [Accessed: January 25, 2024]

[13] A year of war. Frank's Diary 1917—1918 [Internet]. 2023. Available from: https://ayearofwar.com/site-information/ [Accessed: January 25, 2024]

[14] Duffield A. The Post Office during WWII [Internet]. 2019. Available from: https://www.postalmuseum.org/blog/the-post-office-during-wwii/ [Accessed: January 25, 2024]

[15] Crowley MJ.'The Royal Mail Will Always Get Through'—Maintaining Communications on the Home and Military Front during the Second World War [Internet]. 2017. Available from: https://www.researchgate.net/publication/309240800_The_Post_Office_Will_Always_Get_Through_Sustaining_National_Communications_during_the_Second_World_War/link/5ba14a72a6fdccd3cb61efed/download [Accessed: January 25, 2024]

[16] Morshed SMS. Muktijuddhe Dak Bivag (Post Office in Liberation War). Dhaka: Pallik Sourov; 2022

[17] AlJazeera. As War Drags on, Ukraine's Postal Service Perseveres [Internet]. 2022. Available from: https://www.aljazeera.com/news/2022/8/30/as-war-drags-ukraines-postal-service-perseveres [Accessed: January 25, 2024]

[18] Goldstein SH. Postal service, other agencies learned from anthrax attacks in mail. Homeland Defense Journal. 2004;**2**(2):25-30. Available from: https://www.ojp.gov/ncjrs/virtual-library/abstracts/postal-service-other-agencies-learned-anthrax-attacks-mail

[19] Conolly-Smith P. "Reading between the lines": The Bureau of Investigation, the United States post office, and domestic surveillance during world war I. Social Justice. 2009;**36**(115):7-24

[20] Feroze, S. That Unsung 'Philatelic War' ... [Internet]. 2014. Available from: https://www.thedailystar.net/that-unsung-philatelic-war-55642 [Accessed: January 25, 2024]

[21] Zarakol A. States and ontological security: A historical rethinking. Cooperation and Conflict. 2017;**52**(1):48-68. DOI: 10.1177/0010836716653158

[22] Universal Postal Union. Constitution of the Universal Postal Union [Internet]. 2021. Available from: https://www.upu.int/UPU/media/upu/files/aboutUpu/acts/01-actsConstitution/actsConstitutionConsolidatedVersionAmendedInAbidjan2021En.pdf [Accessed: January 25, 2024]

[23] Global Fire Power. 2023 Military Strength Ranking [Internet]. Available from: https://www.globalfirepower.com/countries-listing.php [Accessed: January 25, 2024]

[24] Universal Postal Union. 2022 Postal Development Report: Postal Journey towards a Sustainable Future [Internet]. Available from: https://www.upu.int/UPU/media/upu/publications/postalDevelopmentReport2022.pdf [Accessed: January 25, 2024]

[25] Bluman AG. Elementary Statistics: A Step by Step Approach. 6th ed. New York: McGraw-Hill; 2007

[26] Choi J, Peters M, Mueller RO. Correlational analysis of ordinal data: From Pearson's r to Bayesian polychoric correlation. Asia Pacific Education Review. 2010;**11**(4):459-466. DOI: 10.1007/s12564-010-9096-y

[27] Foddy WH. Elementary Applied Statistics for the Social Sciences. NSW: Harper & Row (Australasia) Pty Limited; 1988

[28] United States Postal Service. Military Mail [Internet]. 2023. Available from: https://about.usps.com/strategic-planning/cs09/CSPO_09_048.htm#:~:text=The%20Department%20of%20Defense%20is,of%20Defense%20around%20the%20world [Accessed: January 25, 2024]

[29] United States Army Human Resources Command. Military Postal Service Agency (MPSA) [Internet]. 2023. Available from: https://www.hrc.army.mil/content/Military%20Postal%20Service%20Agency%20(MPSA) [Accessed: January 25, 2024]

[30] British Forces Post Office. About BFPO [Internet]. 2009. Available from: https://web.archive.org/web/20100330073756/http://www.bfpo.mod.uk/aboutbfpo.htm [Accessed: January 25, 2024]

[31] Randolph J. Communication and obligation: The postal system of the Russian empire, 1700-1850. In: Franklin S, Bowers K, editors. Information and Empire. Mechanisms of Communication in Russia, 1600-1850. UK: Open Book Publishers; 2017. pp. 155-183. Available from: https://books.openbookpublishers.com/10.11647/obp.0122/ch5.xhtml

[32] Roberts PC. Alienation and the Soviet Economy: The Collapse of the Socialist Era. 2nd ed. California: Independent Institute; 2017

Edited by Sally Burt

National security is being redefined in the 21st century. Rapid advances in technology are reminiscent of the initiation of the nuclear age. As the cyber realm and outer space develop as new domains of international competition, there are new strategies and tools for states to utilize and also defend against. Important elements of national security and some strategies are not new but would benefit from exploration with a fresh perspective. This book seeks to explore some of the changing relationships, the nature of alliances, and the UN to better understand national security in the digital and information age. The framework of international law as applied to new domains and gray-zone activity will also be explored to understand the tactics being used in the current strategic environment. Examining these significant elements of national security with a modern eye provides important insights for policymakers and the public in this new age of national security.

Published in London, UK

IntechOpen

ISBN 978-0-85466-669-0
9 780854 666690