



Retaliating against cyber-attacks: a decision-taking framework for policy-makers and enforcers of international and cybersecurity law

Sozon Leventopoulos · Kosmas Pipyros · Dimitris Gritzalis

Received: 16 December 2023 / Accepted: 7 February 2024
© The Author(s) 2024

Abstract Cyber warfare is a reality taking on increasing importance. Governments, state-sponsored actors, and non-state sponsored actors have used cyber-attacks as the “weapon of choice” due to their specific characteristics. Cyber-attacks can be highly targeted and focused, even tailored to a specific unit or system, providing limited to no physical destruction (unlike a cruise missile) and potentially resulting in no loss of life. There are several incident response frameworks and approaches that an organization can implement to enhance its security posture. Usually, these will address specific adverse events such as computer security incidents, which in turn are limited in scope and coverage, typically within an organization. Nations have made limited effort in confronting severe cyber-attacks targeting and/or threatening them, as well as in preventing these attacks from being launched. In this work, we identify and discuss a decision-taking framework that may allow state actors to adopt new options against severe cyber-attacks, not always complying with international norms. Such options are neither encouraged nor supported. On the contrary, we discuss them so that the international community is made aware of such potential frameworks. More specifically, by defining clear thresholds, roles, and responsibilities, by introducing a structured chain of command, and by identifying the potential

Sozon Leventopoulos · ✉ Dimitris Gritzalis
Dept. of Informatics, Athens University of Economics & Business, Athens, Greece
E-Mail: dgrit@aueb.gr

Sozon Leventopoulos
E-Mail: sleventopoulos@aueb.gr

Sozon Leventopoulos
Zonos Systems Consulting, Athens, Greece

Kosmas Pipyros
Dept. of Computer Science, Philips University, Nicosia, Cyprus
E-Mail: pipyros.k@philipsuni.ac.cy

of certain actions, policy makers can recognize an extended decision space that may lead to unpredictable deterrence options against cyber-attacks.

Keywords Cyber-attack · Cybersecurity · Cybersecurity law · Cyber warfare · Deterrence · Incident response · International law · Retaliation

1 Introduction

On September 11, 2001 (9/11), four civilian airplanes were used as “guided bombs” in a coordinated suicide attack [1, 2]. Three of the airplanes were hijacked and crashed on various landmarks, such as the World Trade Center in New York City and the US Pentagon. The fourth airplane crashed in Pennsylvania, after a failed attempt by the passengers to regain control. In response to these attacks, a series of measures and actions were discussed and adopted at the NATO Prague Summit in 2002 [3]. Inter alia, NATO introduced the RENEGADE concept, which provides a structured way for National Authorities to address similar events promptly and effectively. The concept includes provisions regarding effective communication between the various stakeholders, clear roles and responsibilities, and actions which are automatically initiated when certain thresholds are reached.

Over the past decades, cyber-attacks (or cyber offensive operations) [4] have proved their ability to shut down nuclear centrifuges [5], inflict catastrophic failures in power generators¹, or attack military networks. Today, cyberspace is not only considered the 5th domain of operations², but also creates a connection with all the rest of operational domains (i.e., land, sea, air, space). This has shifted the focus from mission assurance to information assurance, and has introduced kinetic warfare jargon (e.g., maneuver, superiority, dominance, etc.) into cyberspace operations. Information assurance requires understanding the relationship between military operations and the need for credible information flows and accurate information products. In that view, managing and responding to risks related to these flows and information is critical for maintaining the initiative in kinetic warfare missions.

Modern military operations conducted within the virtual boundaries of cyberspace are the norm and not the exception [6], and their results extend out to the physical domains. By default, warfare is an unpredictable, chaotic, and non-linear environment, where for years the “fog of war” was inevitable [7]. The advances in micro-electronics and programming languages and the introduction of the Internet have created an overflow, an abundance of information, where billions of devices collect, process, and store a vast amount of data.

¹ In 2007, the Idaho National Laboratory (<https://inl.gov/>) conducted an experiment called “Aurora Generator Test”. The aim of the test was to demonstrate how a cyber-attack could destroy a physical generator, thus underpinning the importance of cybersecurity in industrial infra-structure. The case was de-classified in 2014 (<http://s3.documentcloud.org/documents/1212530/14f00304-documents.pdf>).

² U.S. Dept. of Defense Strategy for Operating in Cyberspace (2011) <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.

1.1 Current situation

It took less than 2 years from the events of 9/11 until the introduction of the RENE-GADE concept. In the meantime, cyber-attacks and cyber warfare operations have been conducted for at least three decades and yet no comparable framework has been widely recognized or implemented. The term cyber-attack is defined here as a deliberate attempt by individuals or organizations to breach the information system of another individual or organization. On the other hand, cyber warfare operations encompass both offensive and defensive cyber maneuvers enacted by military units or state-supported hacker groups to defend or undermine national interests. The key distinction between the two lays in the application: cyber-attacks might serve as elements of cyber warfare, but cyber warfare itself is deployed more broadly, targeting state actors in conjunction with traditional military actions. Detailed insights into cyber warfare are provided in Sect. 2.4. Most of the available playbooks, concepts, plans, and more, deal with how incidents are being handled, and with the responsive actions required in order to quickly restore the status quo ante. None of these documents address cyber-attacks as parts of a larger military campaign. Therefore, these playbooks end with resolving the issue and mitigating the effects.

Our work draws its inspiration from the RENEGADE concept and addresses what could follow a cyber-attack. While responsive actions to the incident or incidents are an internal part of the framework, they are not the end, and a certain path ultimately leading to potential responsive actions is described. In that view, we identify—but without adopting, encouraging, or proposing—a new approach by creating an automated process which connects the sensor³ to the decision taker⁴. By doing that, the international community is made aware of a number of new options that—although not essentially complying with current international norms—are enlarging the available responsive actions decision space for state actors and policy makers.

1.2 Scope and purpose

Cyber warfare is a reality that will take on increasing importance in the following years. Cyber-attacks could be used as the “weapon of choice” due to their specific characteristics. They can be highly targeted and focused, tailored to a specific unit or system, and can result in no or limited physical destruction, and—potentially—no loss of life. Whether or not a State should refrain from cyber-attacks as a retaliation method is heavily dependent upon several criteria. While cyber-attacks and cyber warfare operations have been conducted for decades, still no comparable concept has been introduced or adopted. Current strategic guidelines and operational plans

³ In military operations, a sensor is a device, system, or individual designed or trained to detect, track, or identify targets, providing critical information for situational awareness, threat assessment, and decision-making.

⁴ In the context of military operations, a “decision taker” refers to an individual, typically within the chain of command, who is responsible for making critical judgments and choices based on available information, often under pressure, to determine the course of action in response to strategic, operational, or tactical situations. For further details please see https://irp.fas.org/doddir/dod/jp3_12.pdf.

are primarily concerned with the management of the cyber-attacks and detail the necessary actions to quickly revert systems to their pre-incident condition. However, these documents do not recognize that cyber-attacks may be part of a wider military campaign.

This research paper draws its inspiration from the RENEGADE concept and addresses what should follow a cyber-attack. The purpose of this paper is to propose a novel decision framework and flowchart, which will guide the decision-making process related to retaliatory actions within the concept of cyber warfare. By defining clear roles and responsibilities, and introducing an Attribution–Severity Matrix schema, it creates an automated process which connects the sensor to the decision taker. Doing so generates credible options and increases the decision space. We have followed a human-centric approach that is based on extensive analysis of historical and practical examples, exploiting knowledge acquired by other principles and examples. Furthermore, due to the novelty of this proposal, extensive testing and fine-tuning will be required.

In the following section, the multifaceted nature of warfare is analyzed, as well as cyber warfare, as a means to achieve strategic and operational goals. Furthermore, the transformation of military operations due to technological advancements, particularly in the area of cyber warfare, is explored. Afterwards, in Sect. 3, the research is focused to a structured approach to respond to cyber incidents, highlighting the importance of a rapid and informed reaction to minimize the impact of such events. Moreover, it proposes a framework that addresses the challenges of attributing cyber-attacks to specific actors and emphasizes the necessity of developing response plans that may not always align with international standards. Moving forward, Sect. 4 outlines the application of deterrence theory to cyberspace as a potential tool for preventing cyber-attacks by highlighting that while cyber deterrence may build on traditional deterrence concepts, it necessitates a nuanced approach considering the unique challenges of cyberspace. Finally, Sect. 5 examines the International and European legal frameworks that govern state behavior in cyber-space and ascertains that the established principles and norms of maintaining peace and security, protecting human rights, and ensuring the resilience of critical information infrastructure against cyber threats are aligned with the proposed framework. The concluding segment of the article acknowledges that the traditional deterrence models may not be applicable in cyberspace, due to difficulties in measuring effectiveness and the risk of misinterpretation of escalation following a cyber-attack. The described framework aims to align with international law and military doctrines addressing these challenges.

2 Background

2.1 War and warfare

War is usually the result of the failure of states to resolve various disputes through diplomatic means. Thucydides identified fear, honor, and interest as the root causes of interstate conflict [34]. Usually, war is not the main tool for dispute resolution over

conflicting interests. State power is formulated through diplomatic, international, and economic means prior to resolving to military ones. When the use of force is required for the preservation or manifestation of a nation’s interests, then the military means become predominant, and war becomes a reality [7].

Warfare refers to the strategy, tactics, and means used in armed conflict against an opponent [8]. Essentially, it refers to the methods and strategies employed in waging war. According to Keegan, war is a phenomenon that occurs universally, and its nature and extent are determined by the culture that engages in it [9]. From that perspective, it is evident that battle undergoes constant transformations, although the essence of war stays unchanged. The nature of warfare is primarily influenced by social, diplomatic, political, and technological advancements. Military operations consist of the means of utilizing military forces to achieve strategic and/or operational objectives, through the design, organization, consolidation, and conduct. Through the art of military operations (or operational art), the military commander captures the way in which he will achieve the strategic objectives, and through the operational planning and conduct of the operations he materializes it, connects it with, and integrates it to the appropriate tactical actions to achieve strategic goals. Through military operational art, the efficient use of forces, space, time, and information is of essence. Operational art is not just about processes and techniques but incorporates ideas and concepts alike and combines together all the factors that can influence both the design and conduct of military operations.

Concrete military actions are a method to express the various forms of warfare. The following levels of warfare link the tactical actions required to achieve national objectives:

Strategic level At this level, the national (or multinational objectives in case of an alliance or coalition) guidance that addresses strategic objectives and end states is formulated. The national resources in support of these objectives will be determined, developed, and used at this level.

Operational level Here, the strategy and tactics are linked as needed to achieve the military end-states and strategic objectives. The focus falls on the planning and execution of operations via the Operational Art.

Tactical level Battles and engagements are planned and executed at this stage, to achieve military objectives. Activities focus on the ordered arrangement and maneuver of combat elements in relation to each other and the enemy, to achieve

Table 1 Military operational levels

Military level	Actions
<i>Strategic</i>	Drafting national policy Theater strategy overview
<i>Operational</i>	Design campaigns Design major operations
<i>Tactical</i>	Conduct battles Conduct engagements Small units/crews actions

the relevant objectives. The following table (Table 1) illustrates the various warfare levels along with their relevant characteristics.

2.2 A new form of warfare

The concept of a “revolution in military affairs” first appeared in the Soviet Union (today Russian Federation) in the early 1980s, when Ogarkov wrote about a “military technical revolution” [10] that could dramatically improve lethality as well as the capabilities of conventional weapons⁵. For years, the Soviet doctrine regarding the military technological enabler favored mass production over quality, while the US (mostly) and its allies relied on technological advancements, especially in the fields of micro-electronics and communications as their competitive advantage in the battlefield. In a Congressional hearing in 1970 General Westmoreland testified that “*data links, computer assisted intelligence evaluation, and automated fire control...*” will be used in the future to search for, lock-on, and engage enemy forces.

Information Technology is considered a key enabler in the revolution in military affairs (RMA) and has been materialized in the “system of systems” approach by the US military⁶. To create the required command structures across all services and authorities together with the integration of all weapon-delivery platforms, it is essential to have a robust, reliable, and effective Command, Control, Computers, Communications, and Intelligence (C4I) system. The latter is heavily dependent on information technology advances and efforts. In that view, today’s military forces’ dependence on complex and unreliable systems (e.g., computers and communication systems) that are prone to attacks or disruption(s) begets the risk of a complete breakdown, if these attacks come to materialize and succeed. As a result, the “all-domain warfare” was introduced, where all previously unlinked domains, land, sea, air, space, and cyberspace were now interconnected and inter-dependent.

Hybrid warfare as a term, was proposed by Hoffman [11] and describes a combination of conventional warfare, irregular warfare, and cyber warfare together with information warfare actions, like fake news, disinformation, misinformation, etc. Hybrid warfare has no universally accepted definition. Nevertheless, it helps better understand today’s military operations and the challenges that have emerged. In such a form of warfare all efforts, including conventional military operation, are subordinate to an information campaign. It should be considered as a “whole-of-government” activity. As per the NATO definition⁷ “*hybrid threats combine military and non-military, as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, and deployment of irregular armed groups and use of regular forces*”.

⁵ <https://csbaonline.org/uploads/documents/2002.10.02-Military-Technical-Revolution.pdf>.

⁶ <https://apps.dtic.mil/sti/pdfs/ADA394313.pdf>.

⁷ https://www.nato.int/cps/en/natohq/news_183004.htm.

2.3 Cyberspace

Cyberspace is a global domain of international significance that extends far beyond the domain of internal affairs of any state. Crucially, the uses and abuses of this complex borderless virtual space impinge on vital state interests in the physical world, including national security, public safety, and economic development. An early definition of cyberspace in the military domain was first introduced in the 2000s in the Joint Publication 1-02 [8]. The definition provided then has already been identified as insufficient.

Kuehl defines cyberspace [12] as a “*global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies*”. The increasing importance of cyberspace for military operations has led to the US Department of Defense classifying it as the “5th domain of Warfare”.

2.4 Cyber warfare

While there is an ongoing debate [13] between the various stakeholders on whether the cyber-domain is, or is not, the 5th domain of military operations, many countries are becoming meaningfully engaged with the offensive possibilities that cyberspace can offer. The rise of cyber arming of states is emerging with the establishment of Cyber Military Units all around the world. Furthermore, the explicit references in the National Cyber Security Strategies (NCSS) of most of the EU and NATO member states that their cyber units are mandated to focus on offensive cyber operations leaves no room to doubt that we are at the crossroad of the “cyber-warfare age” [14].

Cyber warfare can be defined as the use of digital attacks against a state with the possibility to cause comparable harm to traditional kinetic warfare by the disruption of vital information, communication systems, and infrastructure [15]. Cyberspace is not sine qua non for the conduct of cyber warfare operations [13]. An insider threat, a spy with physical access to the server, or rogue materials can be used to launch cyber-attacks without the need for cyberspace. Furthermore, kinetic attacks materialized with a cruise or ballistic missiles and targeting data centers and similar infrastructures can also be utilized [6]. The integration of Cyber Military Units into military affairs and the militarization of cyberspace bring new challenges to the surface⁸.

2.5 Incident response

Today’s incident response and recovery workflows and frameworks require that computer security incident response become one of their most important components. The term “incident response” refers to the processes and technologies that an

⁸ https://irp.fas.org/doddir/dod/jp3_12.pdf.

organization should implement for detecting and responding to attacks originating from cyberspace and/or related to cybersecurity. Incident response builds upon two pillars: the first is preventing cyber-attacks, and the second is minimizing the effect if these attacks are to be materialized. While modern risk assessment frameworks can minimize the number of cyber-attacks or minimize their effects, not all incidents can be prevented, or their impact can be accurately calculated. Therefore, it is necessary for organizations to create incident response capabilities for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses and vulnerabilities exploited, and restoring IT services [16].

An *event* is anything that we observe in a system or computer network. Events can vary from user's logging in to a server, sharing a file, requesting a web page, or a security system blocking a connection attempt. Events are not necessarily bad, and indeed not all events have malicious intent or purpose. On the other hand, *adverse events* are those that have a negative impact on any given system. These events may include unauthorized access or use of system privileges, execution of malware, power failures, etc. According to NIST SP 800-61r2 [16] "*a computer security incident is a violation (or imminent threat of violation) of computer security policies, acceptable use policies, or standard security practices*". This definition implies that the relevant policies, standards, and procedures are in place so their violation can be measured.

There are several benefits behind the need for incident response planning, such as systematically responding to computer security incidents, minimizing loss of information or disruption of services, supporting the lessons learned process, etc. Although there is a large number of incident management models and frameworks, they all share some basic characteristics, such as identification, analysis, determination, and application of the proper countermeasures, finally ensuring that the same (or similar) incident will not happen again (part of the lessons learned process). The latter is based upon the notion that the organization had taken all the steps necessary to mitigate the vulnerabilities associated with the security incident and address the relevant risks. This approach usually leaves the offender untouched, either because the organization lacks the relevant digital forensic techniques or because it is impossible to attribute the cyber-attack to a person or individual, or finally, because there are state-backed player(s) involved. Furthermore, current frameworks do not address nation-wide major events (e.g., distributed denial-of-service [DDoS] attacks against Estonia [2007], the Ukrainian–Russian conflict [2022+], etc.).

3 The framework

3.1 Introduction

A State requires a structured and well-defined approach to resort to responsive actions against cyber incident(s). Such an approach can minimize the time gap between the sensor and the decision taker, thus providing credible options for the relevant actions and decisions. While a global effort to regulate actions within cyberspace is under way, most of the relevant efforts are drawn towards cybercrime and the pro-

tection of Critical Infrastructures or Critical Information Infrastructures, leaving acts of aggression untouched. This reality creates a gap between what state-sponsored actors can achieve, and the actions that the affected State can undertake to respond.

In this respect, state actors' responsive plans may be developed and tested—though not necessarily complying with international standards and norms. This work aims at identifying, analyzing, and making publicly known such a potential responsive action, so that the research community can study it as an option, and the international community is made aware of it and be able to build an informed decision on how to address it. In any case, the view of this work should not be considered supportive of such an option.

3.2 Attribution matrix

One of the main issues related to cyber-attacks is that it is hard, if at all possible, to attribute them to certain groups or state-sponsored actors. Moreover, it is feasible for skillful individuals to incorporate key or buzz words. For example, the “Sandworm” group, a highly sophisticated and covert cyber espionage team, attacking military networks in the early 1990s, including the Black Energy attack on Ukrainian power grids, NotPetya ransomware outbreak, etc. The name “Sandworm” was attributed to this group by researchers due to references in their malware code to Frank Herbert's science fiction novel “Dune”. The choice of this name reflects the group's sophisticated and elusive modus operandi, akin to the fictional creature's ability to move unseen through the sand and strike without warning. Further, it is possible for the attackers to add different characteristics in each layer of their attack. The Olympic Destroyer malware, which was used to attack the IT infrastructure in support of the Winter Olympic Games could easily be identified as attribution nightmare⁹. Initially, indicators in the Olympic Destroyer malware code suggested links to several well-known state-sponsored groups, including the Russian-linked Sandworm and North Korean hackers. The malware had intricate false flags—deliberate misdirection embedded in the code—that made attribution challenging. These false flags included

Table 2 Attribution levels

Attribution	Description
<i>Low</i>	Attribution is impossible, misleading, or irrelevant. Such cases might include variable attribution indicators. A proposed threshold here is when evidence leads to at least two different origins or advanced persistent threats (ATP) or to a complex background infrastructure ¹
<i>Medium</i>	Attribution is possible (a proposed threshold would be only one origin or ATP) or clear (clear TTP ²), but the required time to collect the relevant evidence is estimated to require more than 48 h from the initial alert
<i>High</i>	Attribution is possible, easy and can be done in less than 48 h than the initial compromise indicator. This is typical when cyber-attacks will be used as retaliation to a kinetic attack

¹ <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>

² Usually, malicious actors will try to obfuscate their actions following a variety of methods and practices. They will create a maze of websites, internet routing paths, etc., which is virtually impossible to follow

⁹ <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>.

Table 3 Severity of events matrix

Level	Description	Events
V	Cyber, cyber-physical or kinetic attack that directly impacts, destroys, or disrupts ≥ 1 critical infrastructure (CI), and/or critical information infrastructures (CII), and can lead to extended losses of life and financial damages	Kinetic attack(s). Disruption/destruction of the power grid infrastructure. Disruption/destruction of > 1 CI. Heavy disruption against the health sector. Complete breakdown of the financial sector. Heavy and extended disruptions against the private sector and the supply chain
IV	Cyber or cyber-physical attack that directly impacts, destroys, or disrupts 1 CI, and/or CII, and can lead to loss of life and direct financial damages	Disruption/destruction of the power grid infrastructure. Disruption/destruction of 1 CI. Heavy disruption against the health sector. Disruption of financial activities can lead to significant direct financial damage. Extended disruptions against the private sector and the supply chain
III	Cyber or cyber-physical attack that impacts or disrupts networks and computer systems and can lead to direct financial damages	Disruption of computer networks and systems. Disruption of communication networks. Disruption of health care sector. Disruption of financial activities can lead to financial damage. Disruptions against the private sector and the supply chain
II	Cyber-attack that impacts or disrupts networks and computer systems and can lead to limited financial damages	Minor disruption of computer networks and systems. Minor disruption of communication networks. Disruption of financial activities may lead to financial damage. Minor disruptions against the private sector and the supply chain
I	Cyber incident with limited to no impact	Incident against computer and communication networks and systems. False positives. No effect or disruption

similarities to code previously used by North Korean, Chinese, and Russian groups, making it difficult for analysts to determine the true origin of the attack. Based on this, it is identified that attribution efforts are critical for the retaliation approach and should be initiated at the earliest possible attacking state. To create the necessary background, Table 2 depicts potential attribution levels based on the possibility to acquire enough relevant data.

Fig. 1 Responsive action matrix

		Attribution Level		
		Low	Medium	High
Severity Level	V	Cyber	Cyber	Kinetic
	IV	Cyber	Cyber	Cyber
	III	Cyber	Cyber	Cyber
	II	No	Cyber	Cyber
	I	No	No	Cyber

3.3 Severity of events matrix

Measuring the severity of events is a key factor in deciding whether to respond to a cyber-attack. Table 3 illustrates the proposed severity matrix, which is predicated on the National Cyber Incident Scoring System (NCISS) levels established by the Cybersecurity and Infrastructure Security Agency (CISA)¹⁰.

Further, we propose the following Responsive Action Matrix. The matrix suggests the responsive actions based upon the combination of the severity of the initial (cyber) event and the level of achieved attribution. With that, we can address the time criterion, thus creating the required credible options. Fig. 1 outlines the relevant responsive action matrix.

An explanation of Fig. 1 in accordance with International Law is provided below:

Severity level (I-V) The vertical axis likely represents the impact or potential harm caused by a cyber incident, with Level I being the least severe and Level V being the most severe. This aligns with principles of proportionality, suggesting that more severe incidents may warrant stronger responses.

Attribution level (low–high) The horizontal axis likely reflects the confidence in attributing the cyber incident to a specific actor, with ‘Low’ being uncertain attribution and ‘High’ being certain attribution. Attribution is a key factor in international law for determining state responsibility and the appropriate response.

‘No’ response For Levels I and II under ‘Low’ and ‘Medium’ attribution, the matrix indicates no response, which could be interpreted as either the incident does not warrant a response due to its low severity or the uncertainty of attribution makes a response legally or strategically unviable.

‘Cyber’ response This indicates a digital or non-physical response to a cyber incident, such as cyber defense measures, cyber countermeasures, or other forms of digital retaliation. Under international law, such responses must be necessary, proportionate, and adhere to the principle of non-intervention.

¹⁰ <https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss>.

Table 4 Incident response phases

<i>ALERT</i>	Indicators fed by various sensors (e.g., CIMIC ¹ , HUMINT ² , Security Operation Centers, etc.) of potential attacks initiate this phase. Once the threshold is passed, an initial investigation is executed. The result may be categorized as false positive, therefore further investigation is conducted, to document the actions and the findings and update the relevant database(s) and the initial thresholds. If the incident is categorized as an attack the next phase is automatically initiated
<i>FORMULATION</i>	There are three viable options: a kinetic attack, a cyber-attack, or a combination of the two. The key objective of this phase is to determine the Impact level, based on assessments regarding the attribution potential and severity level. Once the impact level is determined, the incident handling, which has three phases, initiates: containment, eradication and finally recovery. The Impact level may fall into one of the following categories: CAT. V: catastrophic/devastating event, CAT. IV: significant impact and/or losses, CAT. III: considerable impact and/or losses, CAT. II: limited impact and/or losses, CAT. I: no impact and/or losses
<i>RESPONSE</i>	Once the impact level and the severity–attribution matrix are determined, the Response phase commences. Based on the relevant findings there are the following options: <i>I</i> : No further action required. The flow ends with the documentation of actions. <i>II, III, IV</i> : Launch of cyber-attack(s). The final decision lies with certain authorities. An assessment of the result of the cyber-attacks should be conducted to identify whether the goal has been achieved and to measure the effects of the response. This part is necessary to identify potential shortfalls or areas of improvement and also prepare for a potential response from the offended state/actor. <i>V</i> : Launch of kinetic attack(s). This form of attack will be a clear statement and can lead to further escalation from the offending state. Therefore, prior to resorting to such an approach, there should be an assurance regarding the attribution level, which should be HIGH, at minimum. The Head of State (or the Minister of National Defense if required) is responsible for taking such decision

¹ CIMIC: Civil-Military Cooperation² HUMINT: HUMAN INTeLLIGENCE

‘Kinetic’ response This indicates a physical response and is only recommended at the highest severity level with high attribution. Under the Tallinn Manual’s interpretation, a kinetic response is permissible under international law if it adheres to the principles of necessity, proportionality, and distinction. This is particularly relevant if the cyber operation can be considered an armed attack under the law of armed conflict.










The matrix suggests a framework where the response escalates not only with the severity of the incident but also with the confidence in attributing the attack to a particular actor. It is critical that the matrix is accompanied by clear definitions and thresholds for each level of severity and attribution. Additionally, the matrix should be developed with an understanding that any response, particularly at the ‘Kinetic’ level, must be in accordance with international law, which includes respecting state sovereignty and avoiding unnecessary harm to civilians and civilian infrastructure.

3.4 Structure and phases

This Incident Response Framework may include three distinct phases, as per Table 4.

Finally, we identify the required roles and responsibilities and the relevant command and control relationships, to respond to the time criticality, limit the line of efforts, and keep the required communications (which could be severely impacted by the initial event) to a minimum. By enabling the appropriate decision-takers in

Table 5 Roles and responsibilities

Role	Responsibility
	Appointed national legal authority
  	Appointed governmental authority
  	Appointed military authority
 	Appointed technical/cyber warfare authority
<i>Note:</i>	<i>Black:</i> Head of state/sector. Has final decision authority. <i>Red:</i> Highest appointed decision-taking authority. <i>Blue:</i> Technical/administrative support

each level, we implement a “man-in-the-loop” approach, which ensures flexibility and prompt actions, down to the level of military unit/civilian sector. The identified roles and responsibilities are outlined in Table 5. The flow-chart supporting the proposed framework, the roles, responsibilities, and command structures is depicted in Fig. 2.

4 The framework as a potential deterrence tool

4.1 Deterrence theory

The classical deterrence theory can be traced back to the Peloponnesian War (431–404 BC), the famous ancient Greek war between the city-states of Athens and Sparta for the hegemony of the Greek world, and the threat of violence in response to adversary actions [17]. The first formal theories of a—strategic—form of national deterrence emerged during the years of Cold War, even though their routes can be traced back to the 1920–1930s, when the air-power theory was taking shape. In 1962, Kahn had coined the idea of “mutual assured destruction” (or MAD), which was based on the strategy of *rational deterrence* [18]. The latter entails that the threat of using destructive weapons against the enemy is an adequate measure for maintaining peace and stability. The strategy itself is based upon Nash’s equilibrium [19] in which, once armed, neither side has the will to initiate a conflict. As per MAD, second-strike capabilities developed by a nuclear-armed defender will result in the annihilation of both the defender and the attacker.

The basic deterrence theories that were proposed and introduced during the Cold War were heavily based upon the perceived advantage that nuclear bombs could replace costlier conventional forces. The destructive force of those nuclear weapons assured total annihilation in the event of their use, and it is a reality that until today no nuclear weapons were used in an armed conflict. Nuclear capable countries were extremely reluctant to use such weapons and their mere existence (or even suspicion of existence as has been observed in the case of Israel/Palestine) had created a perception of a deterrent effect. Nuclear deterrence remained active even after the end of the Cold War. In 1996, the then-secretary of defense Perry asserted

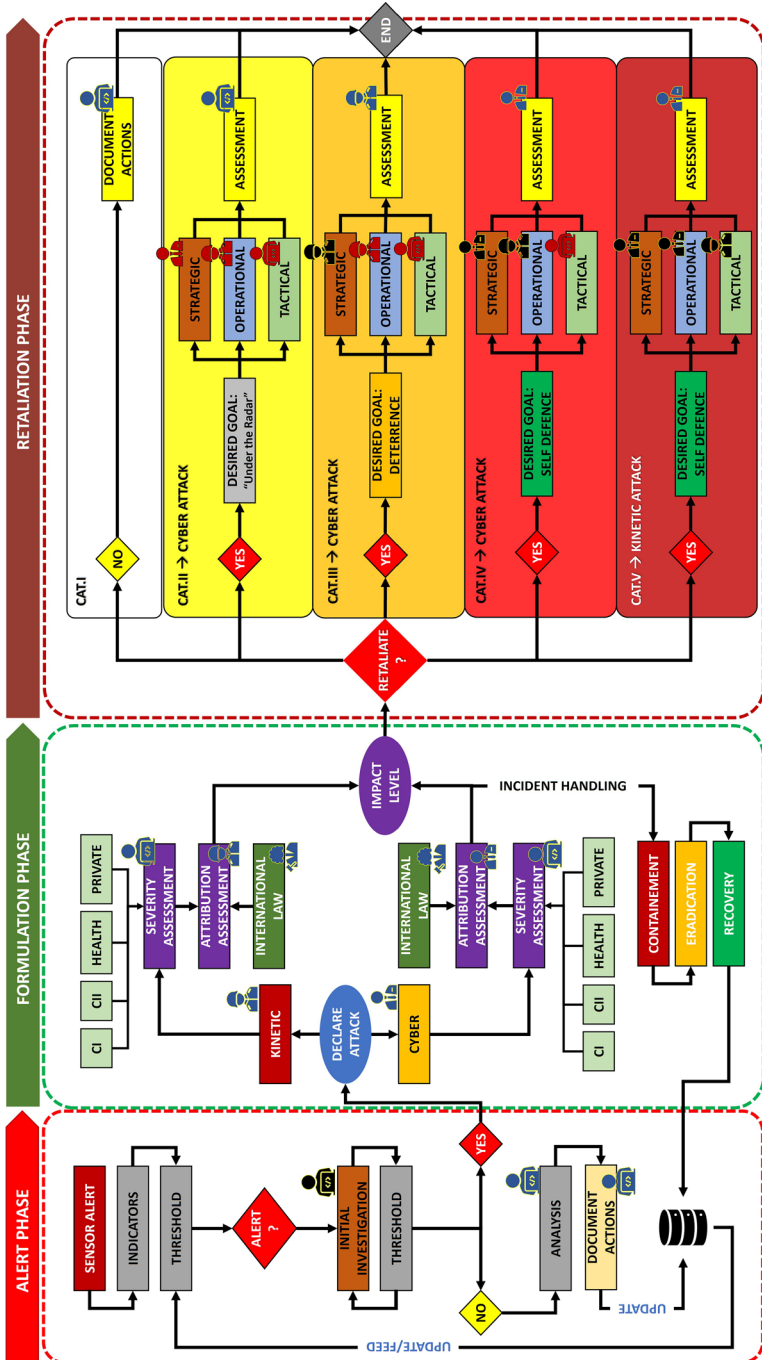


Fig. 2 Incident response framework flowchart

that the US could retaliate with an overwhelming nuclear response against rogue states and other similar powers [20].

The whole deterrence theory can be summarized into the following words, “*if you do this, then I will do to you this plus that*”. In essence, it extends the behavioral modification that is sought through the warfare (ultimately, warfare aims to “persuade” the opponent to accept terms that, under other circumstances, they would be reluctant or unwilling to accept [7]) by increasing the “cost” for the offender. The main difference between warfare and deterrence is that the latter usually works prospectively and not retrospectively. Ultimately, deterrence works within the boundaries of a “cost–benefit” analysis, by increasing the potential “cost” for the offender above its “accepted” level [21]. It can generally be defined [22] as “*the practice of discouraging or restraining someone (...) from taking unwanted actions. [...] It involves an effort to stop or prevent an action*”.

4.2 Deterrence and cyberspace

While deterrence was considered a straightforward concept during the Cold War, and most (if not all) countries embraced deterrence in their national security posture, the concept remains difficult to achieve, even though the “information era” is dominating our economic, social, and personal lives. The wide-scale DDoS attack against Estonia (2007), the Stuxnet case (2010), and a series of events since then gained cyber deterrence more prominence into national security doctrines around the globe, but still the whole concept remains difficult to achieve, since most will focus on preventing (or responding to) attacks on or through cyberspace. Therefore, the majority of the relevant efforts will be directed in resilience rather than deterrence. This is a reasonable approach since the traditional models of deterrence have limited applicability within the boundaries of cyberspace. During the Cold War, a stable bipolar world made the MAD concept possible. Clear communication channels and the relevant perception on international matters led to successful crisis management.

Deterrence has many forms. For example, it can be singular and symmetric, like the nuclear one (or, by extent, the conventional warfare one). If retaliatory actions are to be invoked, then a major conventional or nuclear war is quite possible. Today, there is an endless and constantly changing number of asymmetrical relationships within cyberspace, where stakes, interests, and power all vary and are constantly in flux. In that view, cyber deterrence is considered repeatable and symmetric. Repeatable because, for the time being, it seems not physically possible to eliminate the offending state through cyber-retaliatory actions (unlike nuclear weapons), and symmetric because it could be directed against states and not individuals (peer-to-peer actions). As a result, state entities usually identify three distinct cases of deterrence in cyberspace as their potential actions: (a) cyber-attacks as a retaliatory deterrence method against cyber-attacks, (b) cyber-attacks as a retaliatory deterrence method against kinetic attacks, and (c) kinetic attacks as a retaliatory deterrence method against cyber-attacks.

Table 6 List of requirements for deterrence considerations in cyberspace

Requirement	Consideration
<i>Attribution</i>	It is the process of matching an offender to an offence. It means that the offending state not only has the capacity to determine the source of the attack, but also the capacity is believed and accepted as such by the potential offender. Attribution is a critical element of deterrence, and failure to do so will either be seen as a failure to punish the guilty party, or, if accusing the innocent, as erosion of the legitimacy and legality of the actions. Further in case the retaliatory action is publicly announced (as to enhance deterrence), 3rd parties and the international community together with the State's population need to be convinced of its legitimacy
<i>Capacity to answer</i>	The offended State needs to display credible evidence that it can launch a cyber-retaliatory attack that will, at minimum, match the level of costs associated to the offensive attack
<i>Thresholds</i>	While cyber-attacks can exact a toll of millions in direct and indirect damage, they usually do not harm people, at least directly. Therefore, it might be challenging to address a cyber-attack when the population has not suffered or died from it
<i>Ability to punish</i>	While information technology is present in most of the world today, there are still states that are less dependent upon it. Other states have heavily invested in creating cyber defensive/offensive capabilities that the ability to effectively punish is not always guaranteed
<i>Proportionality</i>	Any action taken that is not proportionate to the original action that triggered the retaliation would automatically be identified as unlawful, thus be considered as revenge. As a rule of thumb, a retaliatory action of the same nature, or similar in nature to the unlawful act against which is directed will be most likely identified as proportionate

4.3 Key considerations

Deterrence is widely considered a fine method, as long as it remains idle. The challenge for a state entity is that the gains from retaliating may be less than the potential counter-retaliation of the attacker. Based on that reality, in comparison to the threat of using nuclear weapons, it was argued [23] that a large-scale conventional war would be more than enough to deter the Soviet Union in the Cold War. The ultimate question is how one can demonstrate a will to retaliate without having to do so, deterring an opponent from acting. The above being said, it might be necessary to further harm critical networks and systems, thus minimizing functionality and usability and increasing the relevant costs, instead of retaliating. Recovery time back to a situation *ante* is also uncertain. Further, the opponent might not only counter-retaliate but—based on the belief that the retaliation was not merited or appropriate, being under pressure to respond, etc.—escalate further. Another option is to respond with a conventional kinetic warfare attack, rather than a cyber-attack, especially if the opponent assumes his inferiority in cyberspace. In the latter scenario, pain and suffering from the kinetic warfare would be far greater than in the case of a cyber-attack-only scenario.

One of the key issues is that retaliatory deterrence in cyberspace needs to be clearly identified. The challenge for a state actor here is that any retaliatory cyber-attack can be lost in the “noise” of modern communications, and the “message” may never be received by the appropriate addressee. Without clear signaling, deterrence may be misinterpreted as aggression. This challenge is not the sole privilege of cyberspace but extends to all the domains [24]. Cyber operations conducted as a de-

terrence method to cyber (or kinetic) attacks from offending peers have the potential to violate international legal obligations. Table 6 refers to a set of prerequisites that need to be considered.

5 Legal considerations

5.1 The international legal framework

Devastated by the two world wars of the last century, nations developed an international regulatory framework that lays down the legal rules, norms, and standards that apply between sovereign states and other entities that are legally recognized as international actors. The United Nations (UN) was established following the conclusion of the 2nd World War and in the light of Allied planning and intentions expressed during that conflict. The purpose of the UN is set out in article 1 of the Charter as follows:

- a) To maintain international peace and security, and to that end, to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which lead to a breach of the peace.
- b) To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace.
- c) To achieve international cooperation in solving international problems of an economic, social, cultural or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion.
- d) To be a center for harmonizing the actions of nations in the attainment of these common ends.

As the main global forum for states to discuss and agree upon issues regarding international security, the UN has been one of the main venues to address international cybersecurity issues. Established to promote international cooperation, the UN is an intergovernmental organization committed to maintaining international peace and security, developing friendly relations among nations, and endorsing social progress, better living standards, and human rights. The UN is based upon the sovereign equality of states and the principles of fulfilment in good faith of the obligations contained in the Charter, the peaceful settlement of disputes and the prohibition on the use of force. It is also provided that member states must assist the organization in its activities taken in accordance with the Chapter and must refrain from assisting states in which the UN is taking preventive or enforcement action [25].

Table 7 List of resolutions and reports related to cybersecurity challenges

Resolution (A/RES)	Title	Summaries
53/70 (1999) ¹	Combating the Criminal Misuse of Information Technologies	The military potential of ICT is mentioned for the first time. The need to prevent cyber-crime and cyber-terrorism is identified. The Resolution invites Member States to inform the Secretary-General on their views regarding definitions and the development of international principles
55/63 (2001) ²	Combating the Criminal Misuse of Information Technologies	The military potential of ICT is mentioned for the first time. The need to prevent cyber-crime and cyber-terrorism is identified. Invites Member States to inform the Secretary-General on their views regarding definitions and the development of international principles
	Combating the Criminal Misuse of Information Technologies	Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairments, and to ensure that any criminal action would be penalized
57/239 (2002) ³	Creation of a Global Culture on Cybersecurity	It recognized that criminal misuse of information technologies can have a significant impact on all states. It calls Member States to incorporate the relevant legal frameworks, and the relevant policies and best practices, in their national legislation
58/199 (2004) ⁴	Creation of a Global Culture on Cybersecurity and the Protection of Critical Information Infrastructures	The resolution identified that the growing number of threats and vulnerabilities in information systems and networks, together with their increasing significance in businesses, organizations and individual users raises new security issues
64/211 (2009) ⁵	Creation of a Global Culture on Cybersecurity and taking stock of national efforts to protect critical information infrastructures	The growing importance of the Critical Information Infrastructures in the societal and economic development was identified
Report A/68/98 ⁶	Developments in the Field of ICT in the Context of International Security	The Resolution recognized that ICT are playing a fundamental role in the information society, thus trust and security should be among the main pillars of their use
Report A/70/174 ⁷	Developments in the Field of ICT the Context of International Security	International law (i.e., UN Charter) is applicable to the cybersphere. State sovereignty applies to the States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory. Existing obligations under international law are applicable to State use of ICT. States must not use proxies to commit internationally wrongful acts using ICT

¹ <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement>

² https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

³ https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

⁴ https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

⁵ <https://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/a-64-211.pdf>

⁶ <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement>

⁷ <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement>

The UN's activities regarding cyber security can be seen as highly fragmented as the subject is addressed in many of its different intergovernmental bodies and organizational platforms. The United Nations Security Council (UNSC) is one of the principal organs of the UN alongside the UN General Assembly (UNGA) and the International Court of Justice (ICJ). The UNSC is intended to operate as an efficient executive organ of limited membership, functioning continuously. The UNSC's main mission is to ensure international peace and security. The UNSC acts on behalf of the members of the organization as a whole in performing its functions, and its decisions are binding upon all member states. Its powers are concentrated in two particular categories, the peaceful settlement of disputes and the adoption of enforcement measures. As one of the most powerful organs, it has the authority to issue binding resolutions to its member states, and—among others—authorize military action.

Furthermore, the UNGA is the parliamentary body of the UN and consists of representatives of all member states. Membership of the UN, as provided by article 4 of the Chapter, is open to “all other peace-loving states which accept the obligations contained in the present Chapter and, the judgment of the organisation, are able and willing to carry out these obligations and is affected by a decision of the UNGA upon the recommendation of the UNSC”. The UNGA has a purely recommendatory role and in that sense, its Resolutions are not binding on the member states. The ICJ is the principal judicial organ of the UN. The Court's mission is to settle, in accordance with international law, legal disputes submitted to it by states and to give advisory opinions on legal questions referred to it by authorized UN organs and specialized agencies (Report of International Court of Justice, A/76/4¹¹). A list of UN Resolutions and Reports related to cybersecurity challenges is provided in Table 7.

5.1.1 Principles and aspects of international law

International law is the law of the international community of states. It is enshrined in conventions, treaties, and standards and it addresses a broad range of domains and issues, like war, diplomacy, trade, etc. It is applied to sovereign states and operated through consent since there is no established way to enforce it. The sources of international law are clearly defined in Article 38(1) of the Statute of the International Court of Justice: International conventions/treaties, international customs, general principles recognized by civilized nations, judicial decisions, and the teachings of the most highly qualified publicists.

Furthermore, it is essential to clarify that international law incorporates two major sets of rules, i.e., *Jus ad bellum*, the body of international law that governs a state's resort to force as an instrument of its national policy (which focuses on the criteria for going to war in the first place by covering issues such as “right purpose”, “duly constituted authority”, and “last resort”), and the *Jus in bello*, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict or international humanitarian law), which governs how warfare is (or should be) conducted [26]. Its main purpose is to limit the suffering caused by

¹¹ <https://www.icj-cij.org/public/files/annual-reports/2020-2021-en.pdf>.

providing protection and assistance to the victims of war by covering issues such as non-combatant immunity and proportionality. *Jus in bello* recognizes the reality of a conflict and regulates only those aspects which are of humanitarian concern. The law of armed conflict is triggered by the existence of aggression, irrespectively of its duration, or how much slaughter is taking place. Its main purpose is to protect combatants and non-combatants from unnecessary suffering and to safeguard the fundamental human rights of persons not actively taking part in hostilities.

A UN General Assembly resolution defined and adopted by consensus the definition of aggression, which is described as the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another State. In 2010, the Rome Statute of the International Criminal Court used this definition in the relevant elements comprising the crime of aggression¹². Article 2 of the UN Charter, forbids the use of force, and asks states to refrain from the threat or use of force in their international relations, with the following exceptions: (a) when the use of force is authorized by the UN Security Council, (b) as an act of individual or collective self-defense if an armed attack occurs, and (c) when Article 5 of the North Atlantic Treaty of 1949 is triggered.

In certain cases, limited use of force is justified, in support of the purposes laid down by the Security Council, but without the Council's express authorization (e.g., Northern Iraq in 1991 and Kosovo in 1999). Finally, it should be stated that the choice of the means and methods of warfare by the parties involved, while it stands as their right it is not unlimited¹³. In that view, the fundamental principles of military necessity, humanity, distinction, and proportionality are still governing the law of armed conflict.

5.1.2 Retaliation and reprisals

The words retaliation and reprisal are not present in the relevant international law treaties. Their exact meaning remains elusive and their scope is considered ambiguous. Article 51 of the UN Charter outlaws both the threat and the use of force and prohibits these acts, unless otherwise authorized by the Security Council, or when States resort to self-defense. Reprisals are a recognized yet controversial concept within international law. They can be defined as “unlawful acts that become lawful in that they constitute a reaction to a delinquency by another state” [27], while Lisitzyn and Kelsen [28] defined reprisals as “acts, which although normally illegal, are exceptionally permitted as the reaction of one state against a violation of its right by another state”. The element of unlawfulness is an essential view of reprisals within the concept of International Law, whereas retaliation can be used in a broader sense, including reprisals, or other unfriendly or hostile, yet lawful acts of retorsion.

The term ‘retaliation’ in International Law is used as a generic one, incorporating retaliation, reprisals, and retorsion [29]. The meaning of these concepts “seem at times to be as varied as the writers dealing with them”. In 1962, Kahn [30] coined

¹² <https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf>.

¹³ On this subject see: Hague Regulations 1907 (HR) Art 22, Additional Protocol I 1977 (AP I), Art 35(1), AP I, Art 36.

Table 8 EU efforts for a legal framework for cybersecurity

	Initiative	Summaries
1	European Program for Critical Infrastructure Protection (EPCIP) ¹	This referred to the doctrine and programs created to identify and protect critical infrastructure that, in the case of fault, incident, or attack, could seriously impact both the country where it is hosted and at least one other European Member State
2	Council Directive 2008/114/EC ² “ <i>on the identification of European critical infrastructures and the assessment of the need to improve their protection</i> ”	An integral part of the EPICP. The Directive aimed to develop common methodologies for the identification and classification of risks, threats, and vulnerabilities to Critical Information Infrastructures (CII) of all EU member states, which eventually would contribute to the protection of EU citizens [31]
3	Commission Communication [COM] (2009) 149 ³ entitled “ <i>Protecting Europe from large-scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience</i> ”	This addressed the protection of CII by strengthening their security and resilience. It focused on prevention, preparedness, and awareness, and proposes a relevant action plan
4	Joint Communication (COM (2013) 1 ⁴) entitled “ <i>Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace</i> ”	The specific Communication presented a proposal for a cybersecurity strategy along with a draft Directive (JOIN, 07.02.2013) addressing Network and Information Security (NIS)
5	The Network and Information Security (NIS) Directive 2013/40/EU ⁵ “ <i>on attacks against information systems and replacing Council Framework Decision 2005/222/JHA</i> ”	The first wide-ranging document dealing with an extensive range of cyber threats. The Directive’s purpose was to create a cybersecurity policy in Europe and a cohesive approach about cybersecurity measures by minimizing discrepancies within and between member states
6	Directive 2016/1148/EU ⁶ of the European Parliament and the Council “ <i>concerning measures for a high common level of security of networks and information systems across the Union</i> ”	The Directive adopted a global approach at the Union level concerning common minimum capacity building and planning requirements to respond effectively to the major threats that cyber-attacks pose to the well-functioning of the internal market

Table 8 (Continued)

	Initiative	Summaries
7	Commission Communication [COM(2020)605] on the EU Security Union Strategy ⁷	The Communication takes a holistic approach to security by providing an overall framework to support national policies and by anticipating and tackling evolving threats whether they are online/offline, digital/physical, or internal/external. It lays the foundations for a security ecosystem that spans the entire breadth of European society. It also addresses the issue of Hybrid Threats and provides a multidisciplinary and integrated response to those threats by helping the EU security stakeholders
8	Directive (EU) 2022/2555 ⁸ of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, (NIS 2 Directive)	The NIS2 Directive is a comprehensive EU-wide legislation focused on enhancing cybersecurity. It updates the existing legal framework in response to the growing digitalization and evolving cyber threats. The directive extends cybersecurity rules to new sectors and entities, bolstering the resilience and incident response capabilities of both public and private entities, as well as competent authorities across the EU. Organizations are mandated to report incidents significantly impacting their service provision. It sets forth cybersecurity risk management measures and reporting obligations for a broad range of critical sectors, aiming to fortify resilience against cyber-attacks, reduce vulnerabilities, and strengthen cyber defense

¹ European Critical Infrastructure (ECI) means an asset, system, or part thereof located on EU territory that is essential for the maintenance of vital societal functions, health, safety, security, economy, or wellbeing of people, and the disruption or destruction of which would have a significant impact on \geq two Member States, as result of failing to maintain those functions [Council Directive 2008/114/EC Articles 2 & 3]

² <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>

³ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN>

⁵ https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2422

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>

⁷ <https://ec.europa.eu/info/sites/default/files/communication-eu-security-union-strategy.pdf>

⁷ <https://eur-lex.europa.eu/eli/dir/2022/2555>

the idea of MAD, based on the strategy of rational deterrence, which holds that the threat of using destructive weapons against the enemy is an adequate measure for maintaining peace and stability. The strategy itself is based upon Nash's equilibrium and dictates that once armed neither side has the will to initiate a conflict.

5.2 The European legal framework

On 8 November 2001, the Committee of Ministers of the Council of Europe adopted the Convention on Cybercrime¹⁴ (also known as the Budapest Convention). Drawn up by the Council of Europe, the Budapest Convention was the first international treaty that addresses internet and computer crime (cybercrime). The Convention was principally aimed at harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime. However, the Budapest Convention did not address concerns that may be raised by cyber-attacks that are not just criminal acts but may also constitute espionage or use of force under the specific legal framework of international law. Table 8 outlines the EU efforts for

¹⁴ <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

a legal framework to protect critical infrastructures from large-scale cyber-attacks and to create an open, safe, and secure cyberspace followed.

6 Conclusions

The advent of cyberspace has introduced a new realm of interaction, transcending traditional physical boundaries¹⁵ [32] and presenting unique challenges to the application of international law. As a domain that is inherently global and decentralized, cyberspace poses significant questions about jurisdiction, sovereignty, and the enforceability of legal norms. Traditional principles of international law, developed in the context of a world divided by territorial borders, face considerable adaptation challenges when applied to the digital landscape. Issues such as cybercrime, data protection, intellectual property rights, and state-sponsored cyber activities push the boundaries of conventional legal frameworks, necessitating a re-examination of how these established norms can be effectively implemented in an online context.

In response to these challenges, there has been a growing movement to develop a coherent set of principles and rules that can govern conduct in cyberspace [33]. This involves not only the adaptation of existing international laws but also the introduction of new legal instruments and cooperative frameworks. States, international organizations, and private entities are engaged in ongoing dialogues to determine how international law can be extended or modified to address the unique characteristics of cyberspace. Key areas of focus include the establishment of jurisdiction in a borderless environment, the balancing of state sovereignty with the global nature of the internet, and the protection of human rights online. As cyberspace continues to evolve, the development of a comprehensive legal framework that respects the complexities of this domain remains a critical task for the international community.

Cyber-attacks have been a reality for more than four decades, and while most military forces have created cyber units, no framework can quickly resolve a decision on whether to retaliate against cyber or a kinetic attack. The described framework appears to build upon the fundamental principles of international law and military doctrines on cyber operations, and identifies key challenges (e.g., attribution, proportionality, termination, etc.). In that view, State actors may argue that it abides by current international law norms and concepts, even though the applicability of international law in cyberspace operations is debatable. For a better understanding of the framework, a severity analysis and attribution matrix were also provided.

In that view, it abides with current international law norms and concepts, even though the applicability of international law in cyberspace operations is still debatable. It also addresses the information overflow, by automating the necessary actions, minimizing command and control communications, and assigning specific roles and responsibilities. In support of the framework, a severity analysis, and

¹⁵ The example of the STUXNET worm and its ability to infiltrate into one of the most heavily armed and protected environments is an example of how cyberspace in general and malware, in particular, can overcome geography and the physical barriers created therein.

a severity—attribution matrix was also proposed. The framework may be further developed and updated by following the proposed steps:

- a) Evaluation through a series of cybersecurity exercises and/or tabletop exercises where the framework can be examined against a series of events and scenarios. The framework can also be evaluated against ad-hoc or legacy approaches. Certain key performance indicators (KPI) can be introduced to measure applicability, flexibility, and effectiveness. A proposed approach is to use the SMART¹⁶ paradigm (Specific—Measurable—Achievable—Relevant—Time-bound) for the identification of the relevant and appropriate KPIs.
- b) Assignment of roles and responsibilities, as well as the establishment of the “command structure” and communication lines needed for its implementation.
- c) Artificial intelligence/machine learning algorithms can also be used to further automate the process and ensure that all the relevant information has been considered. The challenge regarding this option is not the algorithms themselves, but access to valuable and extensive data, ensuring that these data have not been manipulated to create situations where abnormal scenarios would be identified as legitimate actions.

Cyber warfare usually lacks the known components of conventional warfare, such as physical destruction on a massive scale, violence, and submission to another entity’s will. While cyber-attacks might be difficult to be categorized as “armed” ones, the use of cyber capabilities in war is a common feature of today’s conflicts. In that view, the identified framework may be incorporated into the relevant playbooks at the governmental and military levels. It may also be used to allow governmental intervention and enable state authorities to respond to cyber-attacks, even though the latter are directed against the civilian sector. This framework may be adopted by governmental and State use since international law dictates their accountability. It does not apply to corporations and businesses (“hack-back” approach).

Further considerations may refer to the formulation of the relevant thresholds and their consequent update. However, traditional models of deterrence may have little relevance to cyberspace. Moreover, it is difficult to assess the effectiveness of deterrence since there is no baseline behavior to compare with. Cyber-attacks may not even be noticed by the offending state or be misinterpreted, thus leading to escalation. Future research will be focused on developing incident response protocols for states—grounded in international legal principles—that can be practically implemented or clearer mechanisms for the attribution of cyber operations to States considering the technical challenges.

Funding Open access funding provided by HEAL-Link Greece.

¹⁶ S.M.A.R.T. is a mnemonic acronym, giving criteria to guide in the setting of goals and objectives that are assumed to give better results.

Declarations

Conflict of interest S. Leventopoulos, K. Pipyros, and D. Gritzalis declare that they have no competing interests.

Ethical standards For this article no studies with human participants or animals were performed by any of the authors. All studies mentioned were in accordance with the ethical standards indicated in each case.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Moghadam A (2008) *The Globalization of Martyrdom: Al Qaeda, Salafi Jihad, and the Diffusion of Suicide Attacks*. Hopkins. University Press <https://doi.org/10.56021/9780801890550>
- Gilmour, S., Lawrence, W.: *The looming tower: Al-Qaeda's road to 9/11, Policing: A Journal of Policy and Practice*, Volume 1, Issue 1, 2007, Pages 119–121, (2006) <https://doi.org/10.1093/police/pam016>
- NATO (2023) Jan. https://www.nato.int/cps/en/natohq/official_texts_19552.htm. Accessed 2017
- US Dept. of Defense Joint Publications, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf Accessed 20 Jan 2023
- Perlroth N (2021) *This is How they Tell me the World Ends*. London <https://doi.org/10.5038/1944-0472.14.2.1958>
- Defending Ukraine: Early Lessons from the Cyber War: <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/> Accessed 17 Jan 2023
- von Clausewitz C, Al Howard M (1993) *E.: On war*. Everyman, s Library, London
- US Dept. of Defense Dictionary of Military and Associated Terms, https://irp.fas.org/doddir/dod/jp1_02.pdf, Accessed 20 Jan 2023
- Keegan J (1994) *A history of warfare*. Vintage Books, New York
- Herman P The military-technical revolution. *Def Analysis* 10(1):91–95. <https://doi.org/10.1080/07430179408405608>
- Hoffman F (2007) *Conflict in the 21st. Century, The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, Arlington, VA
- Kuehl, D.: *From Cyberspace to Cyberpower: Defining the Problem* (available online: <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf>) Accessed 20 Jan 2023
- Libicki M (2021) *Cyberspace in peace and war*. Naval Institute. Press, USA
- Stiennon R (2016) A short history of cyber warfare. In: Green J (ed) *Cyber warfare: A multidisciplinary analysis*, Routledge Studies in Conflict, Security and Technology. Taylor and Francis, New York <https://doi.org/10.4324/9781315761565-2>
- Singer P, Friedman A (2014) *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press, New York <https://doi.org/10.1093/wentk/9780199918096.001.0001>
- NIST SP 800-61r2: *Computer Security Incident Handling Guide* <https://doi.org/10.6028/NIST.SP.800-61r2>
- (1968) Thucydides and Rex. Warner, “The Sixth Book, Chapter XVIII”. In *History of the Peloponnesian War*. Penguin, Baltimore, MD
- Deudeny D (1983) *Whole earth security: A geopolitics of peace*. Washington. DC
- Osborne M, Rubinstein A (1994) *A course in game theory*. MIT Press, Cambridge
- Keith B (2001) *The Fallacies of Cold War—Deterrence and a New Direction*. Univ. Press of Kentucky, Lexington

21. Freedman, L.: "Introduction—The evolution of deterrence strategy and research," "Deterrence in the 21st century—Insights from theory and practice", F. Osigna & T. Sweijs (eds.), Springer, 2020
22. Mazarr M (2020) In: Osigna F, Swijs T (eds) Understanding deterrence, "Deterrence in the 21st century—Insights from theory and practice". Springer.
23. Mueller J (1991) *Retreat from doomsday: the obsolescence of major war*. Basic Books, New York
24. Schelling T (2020) *Arms and Influence*. Yale University Press <https://doi.org/10.12987/9780300253481>
25. Shaw M (2014) *International Law (Seventh Edition)*. Cambridge University Press
26. Al Corn G (2012) E.: *The law of armed conflict: an operational approach*. New York. Kluwer, Law & Business <https://doi.org/10.1017/S1816383112000781>
27. Cassese A (2004) *International law*. Oxford University Press, p 299 <https://doi.org/10.1093/he/9780199259397.001.0001>
28. Lissitzyn O, Kelsen H (1954) *Principles of International Law*. Columbia Law Rev 54(2):304. <https://doi.org/10.2307/1118738>
29. Colbert E (1948) *Retaliation in International Law*. King's Crown Press, New York <https://doi.org/10.7312/colb92638>
30. Kahn H (1962) *Thinking about the Unthinkable*. Simon & Schuster Inc, New York
31. Pipyros, K., Mitrou, L., Gritzalis, D., Apostolopoulos, T.: A review of obstacles in applying international law rules in cyber warfare, *Information & Computer Security*, vol. 24, no 1, 38–52 (2016). <https://doi.org/10.1108/ICS-12-2014-0081>
32. Kushner, D., "The Real Story of Stuxnet". *IEEE Spectrum*. 50 (3): 48–53. <https://ieeexplore.ieee.org/document/6471059> (2013) accessed 20 Jan. 2023
33. Schmitt M (2017) *Tallinn Manual 2.0 on the International. Law (Applicable to Cyber Operations)*. Cambridge, UK: Cambridge University Press)
34. "Thucydides on Ripeness and Conflict Resolution." *International Studies Quarterly*, vol. 48, no. 1, 2004, pp. 177–95. JSTOR, <http://www.jstor.org/stable/3693568>. Accessed 1 Feb. 2024

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.