National University of Political Studies and Public Administration

DOCTORAL THESIS

Cyber Defence in the Context of Hybrid Warfare. Comparative Study

SUMMARY

Scientific coordinator

Prof. Univ. Dr. Teodor MELEȘCANU

PhD Candidate

Drd. Claudiu-Mihai CODREANU

Bucharest

2022

Table of contents

Summary

Introduction

From the first malware that came to light in the 20th century at the first concerns regarding the prospect of cyberwar (even when it was only a science-fiction topic), from 2007 to the present, cyber operations have become an almost central feature in the actions of state-actors at the international level, cyber means becoming essential for most areas. In 2007, the cyberattacks that paralysed Estonia's digital infrastructure constituted a first, especially because the operation was launched by another state-actor, the Russian Federation. Russia again caused a first in 2008, using cyberattacks within an integrated campaign combined with kinetic operations during the Russo-Georgian War of 2008. However, not only Russia open the way of state-actor deployment of cyberattacks. In 2009-2010, the United States used the Stuxnet malware against Iran, targeting a uranium enrichment facility during an integrated campaign aimed at preventing the Iranian state from developing nuclear weapons. In the following years, cyberattacks started to be integrated in cyber campaigns and integrated within hybrid influencing campaigns which included more instruments. Other first-time events occurred during 2015, namely Russia's cyberattacks against Ukraine's electrical grid and in 2017, alongside Russia's NotPetya cyberattack used against Ukraine, and the global ransomware campaign WannaCry, which had a serious impact on United Kingdom's hospitals. Moreover, in 2020-2021 there were also two major cyber espionage campaigns which provoked significant responses from the United States (the two campaigns were publicly attributed to Russia and China)

State-actors' cyber operations against Euro-Atlantic states have become more and more frequent, but only a part of them can be considered major – those that had significant disruptive effects, were publicly attributed by the affected states, and in some cases they were even the subject of international sanctions. Until present, the Russian Federation employed against Euro-Atlantic states the whole array of cyber operations, from disruptive cyberattacks to cyber espionage. For Russia, Ukraine represented the main target of its offensive cyber operations, taking into account the Russo-Ukrainian War and the hybrid aggressions against Ukraine, but also the Ukrainian state's vulnerabilities. Even though Stuxnet was the first major cyberattack targeting energy infrastructure, the Russian cyberattacks against the Ukrainian electrical grid constituted the first disruptive cyberattacks that aimed at affecting the civilian population. Moreover, the NotPetya cyber campaign caused significant damage in Ukraine and it

represented the cyber operation that produced the costliest damages at a global level. However, a strategic advantage of using cyber operations is maintaining ambiguity regarding the objectives and the responsible actors – features central for hybrid warfare. Thus, states started to strengthen their cyber defence and cybersecurity when state-actors started using cyber operations for political purposes, introducing the first national cybersecurity strategies during the 2000s and beginning to organise their institutions for addressing malicious cyber activities. Euro-Atlantic actors responded to cyber campaigns by collective public attribution of cyber operations and imposing sanctions against the respective states, and by employing their own offensive cyber operations, arguing that they had a defensive aim.

Research design

The main argument of the research is that malicious activities conducted in and through cyberspace, as well as cyberspace on its own, have a major importance for International Relations, as cyber means are integrated in hybrid campaigns used by state-actors. Furthermore, offensive cyber operations deployed by state-actors such as Russia or China are included in a coordinated and integrated campaign of malicious cyber activities, which has the objectives of undermining the states, state institutions, democratic processes and dividing the societies of the targeted states. Therefore, in the context of these hybrid campaigns and cyber campaigns, cyber defence becomes crucial for the security of Euro-Atlantic states, but they should take into consideration respecting democratic values while addressing these developments, as there is also a conflict between democracies and the digital authoritarian model adopted and promoted by states such as Russia and China.

The research tries to answer two main research questions: In what way were offensive cyber operations used by Russia and other state actors against Euro-Atlantic states?; What kind of measures did Euro-Atlantic states implement in order to ensure cyber defence and cybersecurity?. Therefore, the study will be based on two hypotheses:

1. *The major cyber operations deployed by Russia and other state-actors against Euro-Atlantic states are used within cyber campaigns (and they are not isolated incidents) and are integrated inside a series of hybrid instruments and campaigns of influencing and undermining the respective states, characteristic to digital authoritarianism*.
2. *Cyber defence and cybersecurity are central for the efforts of Euro-Atlantic state-actors to respond to hybrid campaigns deployed by Russia and other state-actors.*

In the study of cyber conflict and the ways in which digital technologies are used in political contexts by state and non-state actors, the emphasis started to move away from studying theoretical scenarios that take into account potential "apocalyptic" cyberattacks (such as a "Cyber Pearl Harbor") to scenarios that take into account the reality of continuous low-intensity cyber operations present in various types of conflicts (Dunn Cavelty and Wenger 2020, pp. 14-20). According to Lucas Kello (2017), International Relations (IR) and security studies scholars are sceptical regarding the importance of cyber threats. However, research that links developments from cyberspace, technology and science to politics are not rare anymore in International Relations and security studies (Dunn Cavelty and Wenger 2020, p. 6).

The study will take into account Euro-Atlantic states, analysing the impact of major cyber operations deployed by state-actors against the United States, United Kingdom, Germany and Ukraine. Moreover, the research regarding cyber defence and the discussion regarding national cybersecurity strategies will include the US, the UK, as well as Estonia and the European Union, even though the latter is not a state-actor. For the most part, the research focuses on liberal IR theory, but it takes into account concepts and theories from other IR schools of thought, using a diverse literature from the perspective of IR schools. The case studies represent an exploration of offensive cyber operations deployed against Euro-Atlantic states, following four case studies, similar and different in certain aspects, exploring the unfolding of the cyberattacks, their impact and the manner in which cyber defence was deployed. The cyber operations on which the research focuses consist of those launched by state-actors against other state-actors, but those which were made possible by the Internet, and not only by using digital or cyber technologies.

In order to analyse a cyber operation, the context in which the action occurred should be determined, then there should be determined whether the operations were publicly attributed to a state-actor, whether they had political objectives and affected important instructions and critical infrastructure of the affected state, there should be determined the intensity and complexity of the attack, the impact on the actor's reputation and on society, and also the relation with other events and determining whether the operation is integrated within an extensive cyber campaign or a broader hybrid campaign (Happa and Fairclough 2017; Steiger et al. 2018; Kello 2017). During conflicts between state-actors, cyberwarfare (a set of means used for conducting conflicts in and through cyberspace) can be considered a part or a category of hybrid warfare. Cyber operations are deployed within a larger set of strategies, politics and operations, used as foreign policy instruments and with the aim of undermining the targeted state's security, economy, society or the state itself. This is highlighted by the cyber conflicts

between Russia and Euro-Atlantic states and between China and liberal democracies. Thus, there is a conflict conducted through hybrid means by using cyber instruments (influence operations, sabotage, subversion etc.), but also a conflict between liberal democracies and authoritarian regimes (digital democracy against digital authoritarianism).

Throughout the research, hybrid warfare is understood as a set of means and a manner of conducting conflicts with an extended toolkit. Hybrid warfare represents a blend of different ways of conducting conflicts, it integrates a diversity of different types of conflicts, but it mainly uses non-military means of interference, tailored for undermining the targeted state, for enhancing divisions in the targeted society and weakening cohesion, and hence hybrid warfare represents a strategy or politic of weakening the potential of the targeted actors (Wigell 2019; Lasconjarias and Larsen 2015; Hoffman 2007). Cyber operations are central for hybrid warfare, allowing coercive actions that remain below the threshold of conventional war (Lewis 2015). During this research, I shall use the concept of "hybrid warfare", as in the thesis's title, but also that of hybrid campaigns. Taking in to account the theoretical approaches of Mikael Wigell (2019) and other researchers (Kello 2021; Rinelli and Duyvesteyn 2017; Reichborn-Kjennerud and Cullen 2016; Hoffman 2009; Lasconjarias and Larsen 2015), "hybrid warfare" denotes a set of means, operations, strategies and/or politics through which an actor aims to influence another actor in order to achieve political objectives and to undermine the state or the society.

Furthermore, I have taken into consideration for this research the national cybersecurity strategies of the United Kingdom, the United States, Estonia and the European Union. The UK and the US were selected for this study because they are important state-actors in cyberspace, as the two states were the targets of major cyberattacks in the last 10 years, but they also launched their own cyber operations against other state and non-state actors. Likewise, Estonia was the target of a landmark cyberattack in 2007, and since then the Estonian state significantly focused on developing an efficient and solid cyber defence in order to prevent new attacks, Tallinn representing a model for other states regarding cybersecurity. The EU was also selected because its strategy constitutes the strategy of an international organisation and of a group of states, but also because its state-members were targets of cyberattacks. Moreover, EU's strategy emphasises on online liberties and on advocating for an open and global cyberspace. The discussion regarding the four actors' cybersecurity strategies focuses on the main perceived threats, the ways of action to ensure cyber defence and cybersecurity, and also on the emphasis put on measures such as international cooperation, digital democracy and digital rights. Therefore, cyber defence represents the set of means, politics and measures taken by states in order to prevent or combat cyber operations and cyberattacks. The set includes using

cybersecurity frameworks for critical networks, the development of clear plans for cyber issues and the enhancement of cross-institutional and international cooperation and on measures aimed at boosting the cybersecurity cultures in all sectors.

Thus, the main contributions of this research are analysing the malicious activities conducted in and through cyberspace through an International Relations perspective, analysing the development of the role of cyberspace and cyberattacks for state-actors in the context of the deployment of hybrid means and campaigns. Moreover, the research contributes by analysing the major offensive cyber operations launched by Russia and China against Euro-Atlantic states and integrating them in a coordinated campaign of cyber operations, which is integrated in a hybrid campaign of undermining the targeted states. By discussing the main concepts and theories regarding cyberspace and cyber operations in 1st Chapter, the study contributes at consolidating the understanding of cyberspace, of cyber operations and of cyber defence and cybersecurity in International Relations. Moreover, another contribution for International Relations stems from analysing the major cyber operations deployed by state-actors against Ukraine, US, UK and Germany, consolidating the understanding of the impact of the operations against states and the modalities of response that state can have. Another contribution of the study is improving the understanding of the means trough which cyber defence and cybersecurity can be ensured, especially by advocating models that respect democratic values. The 3rd Chapter focuses on the models of Euro-Atlantic democracies, analysing the cybersecurity strategies of Estonia, US, UK and EU, but also on the digital authoritarian models of Russia and China, and also exploring the UN debate regarding the international regulation of cyberspace and cyber activities, as the UN discussions are the place of confrontation for the two opposing models.

Structure

In the 1st Chapter, the research begins by defining and discussing the main concepts regarding cyberspace (cyber operations, cyberattacks, cyber espionage, cyber weapons etc.), and also on discussing the main aspects of hybrid warfare, the critics against the concept and the concept of cyber war (or conflict). Moreover, the chapter includes an exploration of the main approaches and perspectives regarding cybersecurity from the International Relations field of study, such as discussing the concepts of cyber power, deterrence, international cooperation, the issue of attribution, and digital authoritarianism and the role of state-actors in cyberspace.

The 2nd Chapter explores, for the main part, the major cyber operations that occurred after 2000 and the evolution of Russia's, China's, United States', North Korea's and Iran's cyber operations. In the second part, the chapter also includes an analysis of the major cyber operations deployed by state-actors against four Euro-Atlantic states (Ukraine, United States, United Kingdom and Germany), taking into account the state that had the operation publicly attributed to. The main states that use cyberspace and cyber weapons as means of undermining democracies are China and Russia, but the emphasis is put on Russia's operations, as they are integrated within hybrid campaigns against the targeted states. The research mainly focuses on the cyber operations used against Ukraine's electrical grid, on the NotPetya cyberattack and on the 2016 Russian cyber campaign against US.

The 3rd Chapter follows the way in which a part of Euro-Atlantic states have developed strategies and politics for addressing malicious activities in cyberspace, discussing the main aspects of the cybersecurity strategies of four international actors: United States, United Kingdom, Estonia and the European Union, focusing on the way these four actors plan to ensure their cyber defence and cybersecurity. Moreover, the research also includes a discussion regarding the Russian and Chinese models of cyber defence – the digital authoritarian model – and the debate between digital authoritarianism and digital democracy held at the level of the UN discussions regarding the regulation of cyberspace.

In the 4th Chapter, the study focuses on discussing cyberspace through and IR perspective and its development in the context of hybrid warfare. The chapter includes the analysis of Russia's and China's offensive cyber operations, integrating Russia's operations deployed against Euro-Atlantic states in the means of hybrid campaigns. Moreover, the chapter provides a discussion regarding the cyber defence of Euro-Atlantic states, emphasising on the role of the measures and responses taken, from public attributions to sanctions and to offensive cyber operations and efforts of enhancing cyber resilience and international cooperation. Furthermore, the chapter include a series of recommendations for ensuring cyber defence and cybersecurity.

Findings and discussion

Technologies need to be taken into account as inseparable from politics and vice-versa. Conducting politics in cyberspace produced effects at a global level, creating new interests, interactions and changes in the political discourse, but also new models of global agreements and institutional responses Cyberspace offers new means and areas where states can exercise their power, offering also the possibility of emphasising on sovereignty and territoriality in

justifying their activities. Moreover, cyberspace enabled individuals and organisations to communicate and organise in ways not possible before, which triggered challenges for traditional concepts on sovereignty. (Choucri 2021, pp. 10-14; Dunn Cavelty and Wenger 2022, p. 2)

Therefore, cybersecurity represents a type of security that occurs "in and through cyberspace", and hence cybersecurity practise and constrained and enabled by this environment (Balzacq and Dunn Cavelty 2016, p. 179). Furthermore, Thierry Balzacq and Myriam Dunn Cavelty (2016, p. 183) define cybersecurity as a "set of practices designed to protect networks, computers, programs and data from attack, damage and unauthorised access", the practices being actions taken by different actors for making cyberspace a safer environment. According to Lucas Kello (2017, p. 46), cybersecurity can be understood as the necessary measures for protecting cyberspace from hostile actions, but also as the absence of unauthorised intrusions in computer systems and their well-functioning.

In the context of the debate and confrontation between digital authoritarianism and democracy, liberal democracies seem to have eroded in the last 15 years, whilst digital authoritarianism keeps expanding, becoming more aggressive and offensive. This development was emphasised in the study of the cyber defence and digital authoritarianism model of Russia and China in the 3rd Chapter, but also in the analysis of the cyber operations that targeted Euro-Atlantic democracies in the 2nd Chapter. Russia, China, Iran and North Korea deployed a significant series (or campaign) of cyber operations against Euro-Atlantic democracies, with the objectives of retaliation for different actions of targeted states, but also of undermining the democratic processes, values and institutions, dividing democratic societies, disrupting economic activities and inflicting disruptions for citizens, businesses, civil society or government. Russia deployed all types of cyber operations against Euro-Atlantic states, the majority against Ukraine, from cyber espionage, cyberattacks that produced substantial financial damages and that disrupted that good functioning of critical infrastructure, and others that had the objective of undermining the state and society and the foreign and domestic policy direction of the state (from intrusions, infiltrations, cyber intrusions followed by information leaks and information operations, DDoS attacks etc.). Regarding Russian cyber actions against other Euro-Atlantic states excluding Ukraine, Russia focused on cyber espionage campaigns and cyber operations doubled by disinformation campaigns through which it tried undermining the electoral processes and other features of democracy, undermining public trust in the state and institutions, dividing society and also on altering the direction of the states' foreign policy.

Conversely, China focused on cyber espionage, especially major commercial, financial, industrial and military targets (mainly in the US and NATO states). However, Beijing has not been found responsible for offensive cyber operations with destructive or disruptive objectives, even though several cyber intrusions and infiltrations used in the context of espionage campaigns produced collateral damage. China plays a significant role in cyberspace, both in deploying cyber operations and in its control over technology and over the tech industry, which has a global impact. Beijing chose to mainly use cyber espionage campaigns against Euro-Atlantic states, as disruptive or destructive cyberattacks have been almost non-existent. China frequently uses cyber operations for pursuing objectives related to espionage, extracting sensitive information in order to obtain industrial and commercial advantages. Meanwhile, Russia focused on deploying cyber operations to undermine internal affairs of other states (Kello 2018, p. 666). Even though the intensity of Chinese cyber operations was rather mild, they are nevertheless important, as in the case of the 2020-2021 cyber espionage campaign against the United States (the Microsoft Exchange hack). Therefore, China's cyber espionage campaigns, which mainly targeted the US, are part of an extended campaign and they do not constitute isolated incidents. Moreover, they affect the reputation of the US and they managed to secure the extraction of important data and the operations have a high level of complexity and political objectives, even though they did not have major effects on society, comparable to Russia's cyber campaigns. For instance, the campaigns which exploited vulnerabilities in SolarWinds and Microsoft Exchange constituted cyber espionage campaigns, but the cyber operations that allowed the espionage activities crossed a threshold of acceptability for the US government and its international partners, the operations having a complexity and magnitude high enough to not be tolerated, whilst the backdoors and security flaws created in the development of the intrusions left behind serious vulnerabilities that could have been exploited by any actor with potential destructive objectives. Even though these operations did not have a destructive objective, they constituted in major incursions in critical governmental sectors and accessing significant secret information.

Furthermore, Iran can be considered a significant player in cyberspace, but it deployed far less major cyber operations than China and Russia. Iran focused on cyber espionage and offensive cyber operations launched as retaliation for other actions (such as those against Saudi Arabia in 2012, the US or Israel). Finally, North Korea, a small state with considerable cyber capacities, focused on operations more similar to cybercrime activities, such as ransomware attacks and intrusions targeting bank and financial institutions (having the purpose of extracting funds), but it also launched a major cyber operation against a US-based private company as

retaliation (Sony Pictures). Nevertheless, North Korea was behind one of the most significant, massive and far-reaching cyberattacks in history, WannaCry, a ransomware attack that got out of control and produced collateral damages of billions of dollars, whilst also affecting heavily UK's health system, even though the initial aim of the attack should have been only obtaining ransom from affected organisations.

In contrast, Russia's cyber operations against Euro-Atlantic actors had a clear aim of achieving foreign policy objectives and influence targeted states, its cyber operations and hybrid actions having been perceived as a defence mechanism against adversaries and an attempt of destabilise them. Cyber campaigns allowed Russia to attempt disrupting foreign and domestic policy of a state with the use of non-violent actions, avoiding certain punishments and carrying out the actions below the threshold of war. Cyber operations are deployed with the aim of promoting Moscow's geopolitical aspirations, attempting to distract and destabilize the West to the point that it cannot efficiently respond to Russia's actions, undermining governments and organisations in Euro-Atlantic states perceived as hostile, and also attempting to impose or consolidate its authority in the post-soviet area whilst trying to reclaim its great power status (Limnell 2018, p. 67).

Russian cyber operations deployed after 2007 in Estonia, Georgia, Ukraine, France, Germany, United States, United Kingdom etc. constitute elements of a broader campaign of Russia to weaken public trust, domestic cohesion and the security of European states, but also to undermine the EU and NATO, whilst also raising the costs of pursuing membership of the two organisations (Kello 2021; Wilner 2019). Therefore, cyber operations discussed throughout the 2nd Chapter have been publicly attributed to state-actors, the majority had political objectives, they affected important institutions, democratic processes and critical infrastructure. Moreover, the operations were sophisticated and complex (especially NotPetya or the SolarWinds espionage campaign), whilst the intensity and scale of NotPetya and WannaCry also stands out, they had a significant impact against the affected actors' societies and reputation, and they can be integrated within a broader hybrid campaign of states that promote the digital authoritarian model.

For instance, Russia's cyber operations against the 2016 US presidential elections were complex and sophisticated, they had a high intensity, they undermined liberal democracy, having clear political objectives and managed to inflect a major impact on the state and on society. Moreover, the operations are part of a broader cyber campaign of Russia against the US and other Euro-Atlantic states, and also of a broader campaign of Russian hybrid operations against Euro-Atlantic states, as Russia's malicious activities affected a significant part of these

states while having similar objectives. The operations were doubled by disinformation campaigns and other hybrid means, representing an integrated and coordinated hybrid campaign that aimed at undermining democratic processes, dividing society and interfering in the American elections. In this context, Washington's response consisted in public attributions carried out in international coalitions, imposing sanctions, indictments against several Russian intelligence agents, and deployed its own offensive cyber operations. Russia's hybrid campaign constituted an attempt of dividing US's society and alter the result of the elections, farming a geopolitical environment in which Russia could operate.

Furthermore, Russia's cyber operations against Ukraine were integrated in a broader hybrid campaign against Ukraine, which included the illegal annexation of territories and launching a war in Donbas (including through sending Russian troops and backing separatist forces). Russian cyberattacks against the Ukrainian electrical grid in 2015 and 2016 represented landmark attacks, as well as their level of sophistication and complexity. The operations affected Ukraine's society and it undermined the Ukrainian authorities and the state, as the operation had political objectives. Moreover, the operations were integrated in a broader campaign of cyber operations deployed against Ukraine, from the first attacks against governmental institutions and the electoral process in 2014, to the 2017 NotPetya cyberattack. NotPetya represents one of the most intricate and large scale cyberattacks in history, and also the costliest one. Russia's cyber operations had political objectives, attempting to undermine the Ukrainian state and its economy, affecting the state's reputation, as the attack affected Ukrainian private and public companies (alongside public institutions) and also private companies that were doing business in Ukraine. Furthermore, during the renewal of the Russian invasion of Ukraine in 2022, Russia launched cyberattacks to support its kinetic operations (Microsoft 2022). These cyber operations should be integrated in the context of the whole Russo-Ukrainian conflict, as Russia's objectives seemed to be an attempt to undermine and weaken the Ukrainian state, its society, democracy and economy, similar to other cases. The cyber incidents that occurred in Ukraine achieved the main aim of hybrid warfare, accomplishing political objectives without provoking a response from the adversary through deploying low-intensity actions in order to maintain activities below the threshold of war, offering a constant and intense flow of disruptions of the activities of the Ukrainian government, economy or society (Rõigas 2017, pp. 242-243).

However, Russia's cyber operations in Germany and the UK had a much lower magnitude than those carried out against Ukraine and the US, even though the objectives of cyber interferences in the electoral processes of the two countries were also political. Germany

represented a target of Russian cyber and disinformation campaigns, but the most significant operation occurred in 2015. Since then, Russian interference in the 2017 and 2021 legislative elections has been largely prevented as a result of Germany's substantial cyber defence responses implemented after 2015, such as the public attribution of the 2015 cyberattacks, pursuing dialogue with Russia over these issues, and implemented measures in order to enhance the cybersecurity of electoral processes and public institutions. However, German authorities identified Russian malicious cyber activities in the context of the 2021 elections, they attributed the campaign to Russia, but the activities only had insignificant effects. In the case of the UK, the state has been a target of Russia's hybrid campaign of undermining electoral processes of Euro-Atlantic states, as there are clear suggestions that Russia deployed cyber and disinformation operations during the Brexit campaign, even though the attempts of interference in the 2017 elections were negligible.

Therefore, Russia's major cyber operations were acknowledged at publicly attributed by the US, EU and partner states, and also integrated in coordinated Russian cyber campaigns against targeted states. Moreover, Russia's cyber campaigns are integrated within hybrid campaigns that attempt to influence and interfere the targeted Euro-Atlantic states, as their objectives are the undermining of democratic processes, institutions, and governments, dividing societies, weakening public trust and the disruption of economic activities, of industry and society. Conversely, China focused on significant cyber espionage campaigns that had main objectives of collecting intelligence, even though China's malicious cyber activities are integrated by Euro-Atlantic states within larger cyber campaigns, and they can also be integrated in a coordinated campaign that aims at strengthening and promoting digital authoritarianism (similar to Russia's case). Furthermore, states such as Iran and North Korea represent important actors in cyberspace, but the cyber operations deployed were rather sporadic and did not produce the same effect as Russia's operations, and they did not manage to extract a quantity of important information similar to China's endeavours. However, their cyber operations can be integrated within an offensive campaign of digital authoritarianism, as the aim of their actions is undermining the democracy of targeted states. Authoritarian regimes try to control cyberspace and the information space in order to protect their regimes, whilst also promoting regulations at the global level that correspond to their own visions, and also using digital technologies to control their own populations and to undermine states perceived as adversaries (Barrinha and Renard 2020; Polyakova and Meserole 2018; Yayboke and Brannen 2020). Thus, hybrid interference represents a significant threat for liberal

democracies, as it considers democratic elements as vulnerabilities that can be exploited in order to divide societies and undermine governments (Wigell 2019, p 256).

In this international context regarding cyberspace, Euro-Atlantic states adopted significant objectives of cyber defence, their aim being the strengthening and boosting of cybersecurity. Regarding the cybersecurity strategies discusses in the 3rd Chapter, all four strategies (US, UK, EU, Estonia) had similar perceptions on threats and risks emerging from cyberspace, and all four actors emphasised on respecting democratic values and human rights in elaborating and implementing responses and measures of cyber defence and cybersecurity. The cyber defence and cybersecurity models of the UK and US focus, alongside other measures, on deploying offensive cyber operations with defensive purposes. Moreover, Estonia emphasises on strengthening cyber resilience and international cooperation, whilst the EU focuses on similar objectives to those of Tallinn, as promoting a democratic model of Internet governance and boosting international cooperation with state actors and international organisations are perceived as essential for ensuring cybersecurity at the EU and global level.

Cyber defence and cybersecurity have become central to Euro-Atlantic actors' endeavours of responding to Russia's or other actors' hybrid campaigns. Euro-Atlantic actors work constantly on strengthening their domestic cybersecurity and cyber resilience, but also on boosting international cooperation, both for improving cyber capacities and for offering collective responses against offensive cyber operations, such as collective public attributions or imposing sanctions. Responses regarding cyber threats and cyberattacks do not have to be also in the nature of cyber retaliation, as publicly attributing operations to actors responsible and imposing international sanctions alongside other states had been the preferred response of Euro-Atlantic states after 2015. Moreover, Euro-Atlantic actors attempt to focus on respecting and promoting democratic values, both in developing responses against malicious cyber activities and in promoting a democratic model of governing cyberspace as an alternative to the digital authoritarian model adopted and promoted by China and Russia.

At the most elementary level, cyber defence (or the defence of networks and systems) consists of using antivirus software that automatically scan for malicious codes, and analysts that actively monitor all network activity, whilst also looking for security flaws and intrusions in the networks of potential adversaries in order to obtain intelligence regarding their intensions and capabilities (Buchanan 2016, p. 157). Moreover, states need to carry out a security audit regarding governmental cyber systems and the security of classified networks and systems, as conducting constant analyses is important for detecting vulnerabilities in networks and systems (Polyakova and Boyer 2018, pp. 16-30. In addition to this, Joe Burton and Claire Lain (2020,

p. 16) argue that the concept of critical infrastructure should be expanded in order to include democratic processes, the education sector, social networks and movements and identity groups (ethnic, religious or gender).

Therefore, states targeted by systematic hybrid aggressions should analyse and name such actions as a set of coordinated offensive activities, imposing punishments to the whole strategic campaign and not only to isolated individual actions. States need to take punitive measures against a series or campaign of cyber operations and not only against individual cases, and also to use cross-sector measures in order to respond to cyber operations (financial and economic sanctions instead of individual sanctions, and deteriorate commercial relations), whilst states also need to set a clear message that they have the capacities and will to retaliate in cyberspace (Kello 2021, pp. 12-13). For instance, since 2017 the US and UK started choosing attribution and observing whole campaigns of cyber intrusions and not only the attribution of specific incidents (Egloff 2020, p. 6).

Thus, one of the most important methods of deterrence and response to offensive cyber operations is the public attribution of operations, especially when it is carried out in cooperation with other states. The public attribution of cyber operations has the objectives of coercion and deterrence, ensuring that the adversary has to spend more time and resources on improving its capacities. Moreover, two other objectives are prevention and defence, and the public dissemination of information regarding certain threats can also determine networks' operators to rapidly patch security flaws and ensure a greater resilience of their systems. (Egloff and Smeets 2021, pp. 6-7).

Since 2017 the number of public attributions done by states has increased significantly, including coordinated and collective attributions. States started to publicly attributed cyber operations that had been less significant compared to past cyberattacks, suggesting that attacks similar to those from before 2018 have a greater chance of being publicly attributed and face a more serious response. Moreover, public attribution also constitutes an occasion for states to invoke international law and international norms (including the norms agreed by the UN Group of Governmental Experts) while responding to a cyberattack.

In addition to this, states cannot ensure cybersecurity by themselves, and therefore they should boost their efforts of strengthening international cooperation, aiming at reaching an agreement regarding a sound framework of governing cyberspace and a set of norms for the responsible behaviour of states in cyberspace (Dunn Cavelty and Wenger 2020, p. 23). Moreover, states should support international cooperation, including through frequent exchanges and dialogues with other states, especially in the context of the most important

elections (Polyakova and Boyer 2018, p. 32). States should strengthen cyber resilience at a global level through partnerships with other state actors and regional and international organisations (such as OSCE, NATO, African Union etc.) and also with private actors (Pawlak 2018, p. 113). Thus, states should support alternative dialogue platforms at the international level regarding cyber issues (Pawlak 2018, p. 114). Without significant bilateral agreements, sound measures of consolidating trust or global agreements, even developing communication channels between state actors with major cyber capabilities (such as the US, UK, China and Russia) can contribute to the improvement of the level of security and stability (Buchanan 2016, p. 166).

Taking into account that cyberspace constitutes a cross-border environment that is nevertheless heavily regulated by some governments, intentional cooperation can have an important and significant impact for ensuring cyber defence and cybersecurity. International cooperation is important both for the major states with important roles in cyberspace (the main cyber powers) and for liberal democracies in their endeavours of building their own model and bloc of states that promote digital democracy at the international level, in the context of the development of a bloc of states that promote Russian or Chinese digital authoritarianism. International cooperation regarding cyberspace must be boosted and consolidated, especially within discussions carried out in the UN GGE process. This could be entirely possible, taking into account that actors in cyberspace already cooperate in the case of technical issues, respecting ICANN standards and the main DNS servers or the central infrastructure of the Internet (Nye 2018; Kello 2021). Moreover, states have reached a slight agreement in the UN GGE process, but discussions should be deepened in order to achieve a set of norms accepted and respected by all state actors.

Moreover, even though cyberspace seems to favour cyber offense (Isnarti 2016; Slayton 2017), states should focus on cyber defence and deterrence and advocate for an international regime for cyberspace. Even though the costs of deployed a complex and sophisticated cyberattack are substantial, the costs of cyber defence are even higher (Kello 2018, pp. 68-74). Cyber defenders should always assume that adversaries are already inside the networks that they work on protecting. The US pursued several offensive cyber operations over the last years, but the most significant operations in recent years have been those carried out in the context of the 2020 presidential elections, taking into account the events occurred during 2016 and Russia's interference. For instance, the Stuxnet cyberattack represented a part of a broader campaign of the US, Israel and other international partners to deprive Iran of the ability of producing enriched uranium (Kello 2016, p. 63).

Nevertheless, offensive cyber operations, no matter the state actor that carries them out, leave behind issues for all Internet users. Intelligence agencies are one of the most important actors in cyberspace, especially regarding its strategic manipulation. Besides offensive and defensive cyber operations, intelligence agencies look for and exploit secret security flaws of commonly used software in order to obtain access in different locations inside the Internet's infrastructure. The implants and points of access obtained by intelligence agencies can be used for a variety of purposes, from espionage to disruptive actions, and they can be activated at any time as long as the victims do not manage to detect the vulnerability or the intrusions. However, when it comes to offensive cyber operations, state actors end up endangering their own national security by identifying and keeping secret vulnerabilities, as long as they can also be exploited by other actors. (Dunn Cavelty and Egloff 2019, p. 47)

Furthermore, the main features of liberal democracy, such as political pluralism, media freedom, open economy and the rule of law are perceived and exploited as vulnerabilities through the usage of hybrid interferences. In order to uphold the rule of law and civil liberties, liberal democracies have a limited set of means for addressing cyber and information threats (including those targeting elections), as well as in limiting the activities of extremist parties or of media groups bought or controlled by another actor and actively used for hybrid interferences. However, the vulnerabilities of liberal democracies can be addressed by respecting the same principles of liberal democracy, exactly the inclusive politics and ability of managing changes represent assets for countering hybrid interferences. For instance, non-governmental organisations and social movements can offer efficient democratic mechanisms for monitoring and exposing hybrid interferences, and also media freedom represents a major asset, operating as a monitor of interferences, especially taking into account investigative journalism (e.g., *Bellingcat*) (Wigell 2019, pp. 268-273).

Moreover, states need to work on promoting the culture of cyber resilience and cyber hygiene and also on raising awareness at all levels of society and government (Pawlak 2018, p. 113). However, the efforts and measures from the areas of cyber defence and cybersecurity need to represent foremost the responsibility of the state and its institutions, of private companies from all sectors related to technology and of critical infrastructure operators, and only then the responsibility of the business environment, media, civil society, academia and individuals.

In addition to this, states need to integrate democracy and human rights in efforts related to cybersecurity in order to ensure that the measures respect online liberties and human rights and constitute an alternative to digital authoritarianism (Yayboke and Brannen 2020, p. 7).

Freedom of speech and the right of privacy should be seen as positively contributing to the cybersecurity, taking into account that the amount of unencrypted data would be reduced, which would lead to a drop in cybercrime and cyber espionage (Dunn Cavelty 2014, p. 711). Promoting a safe and free Internet is central to the advancement of a democratic model of Internet governance and cybersecurity that represents an alternative to digital authoritarianism (Yayboke and Brannen 2020, p. 8).

Conclusion

The cyber operations discussed throughout the study significantly affected the targeted states, and a several of them (such as WannaCry, NotPetya or the attack against Ukraine's electrical grid) represented landmark cases even more serious than the 2007 cyberattacks against Estonia. Moreover, the study emphasised Russia's role in its cyber campaigns against Euro-Atlantic states, and the cyber operations were included within hybrid campaigns of influencing and undermining targeted states. In addition to this, the cyber operations deployed by China, North Korea and Iran also had a negative impact on cybersecurity and cyberspace at a global level, and even some of the offensive activities pursued by the United States and the practices of intelligence agencies. Nevertheless, Euro-Atlantic states worked on consolidating their cyber defence and cybersecurity, whilst also taking into account the need of respecting democratic values, human rights and civil liberties, in contrast with the digital authoritarian models of Russia and China. Furthermore, democratic states need to develop and adopt a democratic model for Internet governance in order to counter digital authoritarianism.

Cyber defence in the context of hybrid warfare needs to be integrated within a broader campaign of defending against hybrid warfare's set of instruments, and the responses and measures taken as a result of cyber operations should include a large set of measures, as cyber operations and cyber defence are central, but not the only measures. Furthermore, major cyber incidents triggered by state actors are almost never isolated or singular incidents, as they are in fact integrated by the respective state within a broader cyber campaign and also within a disinformation campaign, an influence campaign, an attempt of changing the behaviour, attitudes and foreign or domestic directions of the targeted states, all of these being means of hybrid warfare. Thus, cyber defence should be implemented in the same way and taking into account the same elements.

Taking into account that the competition between Euro-Atlantic states and Russia has been intensified over the last years (and the same for China), it is expected that cyber operations should raise both in number and intensity in the next period, but also that Russia will exploit

the situation created by the war of aggression against Ukraine for launching new destructive cyberattacks, whilst China will most probably continue its cyber espionage campaigns. Moreover, the continuous development of the Internet and digital means, the continuous digitalisation and the expansion of cyberspace will create new opportunities for cyber operations, as there is also a significant probability that the role of non-state actors will be highlighted in the next period.

Cyberspace is directly affected by conflicts, especially by cyber operations that target critical infrastructure and those that attempt to undermine public trust. At the same time, cyberspace is becoming more and more dependent and interconnected with space technologies, artificial intelligence (AI) and quantic computers, expanding cyberspace and connecting it to more and more sectors of public policy. Moreover, AI will become an essential element of cybersecurity that could have a major impact both on offensive and defensive cyber operations. In this context, the development of the Internet of Things will represent a major challenge for cybersecurity, alongside with the interconnection through the Internet of household appliances, health systems or vehicles. (Dunn Cavelty and Wenger 2020, p. 23; Healey 2019, p. 2; Willett 2021, p. 19)

References

Balzacq, Thierry, and Myriam Dunn Cavelty. 2016. „A theory of actor-network for cyber-security". *European Journal of International Security* 1, no. 2: 176-198.

Barrinha, André, and Thomas Renard. 2020. „Power and diplomacy in the post-liberal cyberspace". *International Affairs* 96, no. 3: 749-766.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations*. New York: Oxford University Press.

Burton, Joe, and Clare Lain. 2020. „Desecuritising cybersecurity: towards a societal approach". *Journal of Cyber Policy* 5, no. 3: pp. 449-470.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge: The MIT Press.

Dunn Cavelty, Myriam, and Andreas Wenger. 2020. „Cyber security meets security politics: Complex technology, fragmented politics, and networked science". *Contemporary Security Policy* 41, no. 1: 5-32.

Dunn Cavelty, Myriam, and Andreas Wenger. 2022. *Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation*. London and New York: Routledge.

Dunn Cavelty, Myriam, and Florian J. Egloff. 2019. „The politics of cybersecurity: Balancing different roles of the state". *St. Antony's International Review* 15, no. 1: pp. 37-57.

Dunn Cavelty, Myriam. 2014. „Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities". *Science and engineering ethics* 20, no. 3: 701-715.

Happa, Jassim, and Graham Fairclough. 2017. „A Model to Facilitate Discussions About Cyber Attacks". In *Ethics and Policies for Cyber Operations*, ed. Mariarosaria Taddeo and Ludovica Glorioso, pp. 169-186. Cham: Springer.

Healey, Jason. 2019. „The implications of persistent (and permanent) engagement in cyberspace". *Journal of Cybersecurity* 5, no. 1:1-15.

Hoffman, Frank G. 2007. *Conflict in the 21st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies.

Hoffman, Frank G. 2009. „*Hybrid threats: Reconceptualizing the evolving character of modern conflict"*. *Strategic Forum*, no. 240: pp. 1-8.

Isnarti, Rika. 2016. „A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War". *Andalas Journal of International Studies (AJIS)* 5, no. 2: pp. 151-165.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven and London: Yale University Press.

Kello, Lucas. 2018. „Cyber Defence". In *The Handbook of European Defence Policies and Armed Forces*, ed. Hugo Meijer and Marco Wyss, pp. 659-672. Oxford: Oxford University Press.

Kello, Lucas. 2021. „Cyber legalism: why it fails and what to do about it". *Journal of Cybersecurity* 7, no. 1: 1-15.

Lasconjarias, Guillaume, and Jeffrey Arthur Larsen. 2015. *NATO's Response to Hybrid Threats*. Roma: NATO Defense College.

Lewis, James A. 2015. „Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine". In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kennet Geers, pp. 39-48. Tallinn: NATO CCD COE Publications.

Limnell, Jarno. 2018. „Russian activities in the EU". In *Hacks, leaks and disruptions: Russian cyber strategies*, ed. Nicu Popescu and Stanislav Secrieru, pp. 65-74. *Chaillot Paper* 148. Paris: EU Institute for Security Studies.

Microsoft. 2022. „Defending Ukraine: Early Lessons from the Cyber War". *Microsoft*, 22 iunie. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Nye, Joseph S. 2018. „Normative Restraints on Cyber Conflict". *Belfer Center for Science and International Affairs*, august 2018. Available at: https://www.belfercenter.org/sites/default/files/files/publication/Nye%20Normative%20Restraints%20Final.pdf.

Pawlak, Patryk. 2018. „Protecting and defending Europe's Cyberspace". In *Hacks, leaks and disruptions: Russian cyber strategies*, ed. Nicu Popescu and Stanislav Secrieru, pp. 103-114. *Chaillot Paper* 148. Paris: EU Institute for Security Studies.

Polyakova, Alina, and Chris Meserole. 2019. „Exporting digital authoritarianism. The Russian and Chinese models". *Brookings*, August 2019. Available at: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Polyakova, Alina, and Spencer P. Boyer. 2018. „The future of political warfare: Russia, the West, and the coming age of global digital competition". *Brookings*, March 2018. Available at: https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/.

Rinelli, Sebastian, and Isabelle Duyvesteyn. 2018. „The Missing Link: Civil-Military Cooperation and Hybrid Wars". In *A Civil-Military Response to Hybrid Threats*, ed. Eugenio Cusumano and Marian Corbe, pp. 17-40. Cham: Springer.

Rõigas, Henry. 2017. „Cyber War in Perspective: Lessons from the Conflict in Ukraine". In *A Civil-Military Response to Hybrid Threats*, ed. Eugenio Cusumano and Marian Corbe, pp. 233-258. Cham: Springer.

Slayton, Rebecca. 2017. „What is the cyber offense-defense balance? Conceptions, causes, and assessment". *International Security* 41, no. 3: pp. 72-109.

Steiger, Stefan, Sebastian Harnisch, Kerstin Zettl, and Johannes Lohmann. 2018. „Conceptualising conflicts in cyberspace". *Journal of Cyber Policy* 3, no. 1: pp. 77-95.

Wigell, Mikael. 2019. „Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy". *International Affairs* 95, no. 2: 255-275.

Willet, Marcus. 2021. „Lessons of the SolarWinds Hack". *Survival* 63, no. 2: 7-26.

Yayboke, Erol, and Sam Brannen. 2020. „Promote and Build. A Strategic Approach to Digital Authoritarianism". *CSIS Briefs*, 15 October. Available at: https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism