CYBERSECURITY

BETWEEN GLOBAL VULNERABILITIES AND REGIONAL REALITIES: CYBERSECURITY DYNAMICS IN EASTERN EUROPE

Dragoș VETRESCU[*]

Abstract:
In the vast, unbounded domain of cyberspace, the concept of regional dynamics often seems overshadowed by its inherent global nature. However, the Eastern European digital landscape presents a compelling case for recognizing and understanding the significance of regional cybersecurity nuances. This article delves into the unique cyber threats faced by Eastern Europe, influenced by intertwined state relations, particularly the pervasive cyber influence of Russia. It highlights shared vulnerabilities resulting from common technological infrastructures, interlinked economies, and mutual dependencies that make the region a collective cyber target. Furthermore, the article discusses the external shaping forces, such as the regulatory influence of the European Union and the strategic involvement of global powers like the US, in strengthening the region's cyber defences. By juxtaposing the global essence of cyberspace with the discernible regional contours in Eastern Europe, this article underscores the importance of a regional perspective in formulating nuanced, effective cybersecurity strategies.

Keywords: *Near-abroad, Cyber security, Regional Security Complex.*

Introduction

Amid the vast, borderless expanse of cyberspace, where geographical markers seem almost redundant, the idea of a regional cybersecurity complex may initially sound incongruous. Cyberspace inherently erases traditional territorial demarcations, presenting a landscape where every node, regardless of its physical location, is equally accessible to threat actors. Given this level playing field, one might assume that cyber threats, devoid of the constraints of physical

[*] PhD student, SNSPA Bucharest, email: dragos.vetrescu.20@drd.snspa.ro

space, would be uniformly global, not bound or majorly influenced by regional dynamics. This presumption finds further backing in the evidence that cybercriminals, hacktivists, or even state-backed entities can orchestrate their operations from any corner of the world, targeting nations irrespective of geography or historical contexts. However, upon deeper introspection, specific regional contours emerge in the cybersecurity landscape, demanding a shift from a purely global perspective to a nuanced regional one.

The Eastern European countries considered by Russia its "near-abroad" offer a vivid illustration of this regional dynamics. Here, the entwined state-to-state relations amplify common cyber threats. The prevalent Russian influence, marked by its persistent and sophisticated cyber campaigns, underscores the unique threat landscape of the region. Such state-sponsored activities, particularly from Moscow, not only underscore the geopolitics of the region but also point to the region-specific cyber threats it faces. States in this region, while participating in a global digital environment, exhibit common vulnerabilities arising from similar technological choices, shared infrastructure, and interlinked economies. Such shared vulnerabilities make the region a collective target, with repercussions in one state potentially rippling through its neighbours.

Furthermore, the intersection of Eastern European states with entities like the European Union shapes its cybersecurity posture. The EU's regulatory norms, especially around cybersecurity, exert a significant influence, harmonizing cybersecurity measures across member states and even influencing non-member neighbouring countries. At the same time, global powers, particularly the US, play an instrumental role, fortifying the region's cyber capacities both bilaterally and under NATO's aegis. The US's dedicated efforts to build cybersecurity resilience in Eastern Europe, from capability enhancement to joint cyber exercises, magnify the role of global powers in shaping the regional cyber landscape.

In essence, while the global nature of cyberspace remains an undeniable reality, regional undercurrents, defined by geopolitics, shared vulnerabilities, and external influences, play a pivotal role in determining the cyber threat landscape of specific areas. Recognizing and understanding these regional nuances can pave the way for more

informed, collaborative, and effective cybersecurity strategies, tailored to address the unique challenges of each region. Eastern Europe, with its intricate web of state relations, external influences, and shared digital dynamics, stands as a testament to the value of conceptualizing cybersecurity through a regional lens.

This article aims to explore the regional cybersecurity dynamics in Eastern Europe, focusing on the intersection of geopolitical influences, shared technological vulnerabilities, and external interventions. Utilizing a theoretical framework grounded in the regional security complex (RSC) theory, the study employs a qualitative analysis of state-to-state cyber interactions, historical cyber incidents, and the influence of major powers, particularly the EU and the US, to understand the unique cybersecurity challenges and strategies within this specific geopolitical context.

What constitutes a Regional Security Complex (RSC)

The theory of the regional security complex is intricately linked to the framework of the English School of international relations. This connection is especially evident in the works of one of its foremost proponents, Barry Buzan. In his seminal work "Regions and Power," Buzan distinguishes between three principal theoretical perspectives on the Post-Cold War international security structure: the neorealist, globalist, and regionalist perspectives (Buzan & Wæver, 2004, p. 6). He particularly gravitates towards the regionalist perspective. While this viewpoint shares certain parallels with the prior two, it differentiates itself based on its regional focus as opposed to a state or global focus. It also varies in its understanding of the mechanisms underpinning security.

The regional perspective as envisaged by Buzan is rooted in his prior research and writings. It adopts a constructivist stance on the emergence and cessation of threats to security. As articulated by Buzan, "the formation and operation of RSCs hinge on patterns of amity and enmity among the units in the system" (Buzan & Wæver, 2004, p. 40). This implies that regional systems are not merely deterministic reflections of power distribution but are contingent upon the actions and interpretations of the involved actors.

Therefore, while the security complex theory retains a significant realist foundation, it also incorporates more liberal concepts (Wunderlich, 2016, p. 39). These include ideas such as security communities and the consequential roles of regional regimes and institutions.

The theory of the regional security complex offers a complementary lens to other international relations theories, enhancing their depth and reducing oversimplification, especially when addressing global issues. By zeroing in on regional dynamics, it provides a more nuanced perspective. The emphasis on the regional level arises from the pragmatic observation that, while there has been a pronounced focus on states as the primary objects of security (Buzan et al., 1998, p. 36), the national security of any state is intrinsically linked to that of its neighbours. As security dynamics are fundamentally relational, the security of any nation cannot be isolated from its surroundings. This idea is encapsulated in the thought that "no nation's security is self-contained" (Buzan et al., 1998, p. 43). In the realm of regional security complex theory, the crux lies in examining the relationships states and societies maintain in terms of vulnerabilities and threats.

Furthermore, as outlined by Buzan and his colleagues, as the international power dynamic becomes "more diffuse" (Buzan et al., 1998, p. 11) and major powers show increasing hesitancy to undertake political commitments in distant regions – unless their core interests are directly and intensely impacted – it's anticipated that international relations will adopt a more regional-centric tone. This shift means regions may increasingly find themselves navigating their challenges more autonomously.

The regional security complex (RSC) theory posits that viewing global security – emphasizing the international system as a whole – as a tangible reality is more an "aspiration than a reality" (Buzan & Wæver, 2004, p. 43). In comparison to the national and global dimensions, the regional level emerges as the critical juncture where these two extremes intersect and witness the most significant activity. Wunderlich underscores this notion, stating, "although all states are enmeshed in a global web of security interdependencies, insecurities are usually associated with geographic proximity" (Wunderlich, 2016, p. 39). Steward-Ingersoll and Frazier pinpoint another rationale highlighting

the primacy of regional security concerns for most states: the simple fact that "most states do not have the capacity to project force beyond their immediate neighbourhood" as "power degrades across distance" (Stewart-Ingersoll & Frazier, 2012, p. 5).

Importantly, security complexes should be perceived as "regions as seen through the lens of security" (Buzan & Wæver, 2004, pp. 43–44). They might not always align with traditional geographic boundaries. This perspective ensures adaptability in the concept of security regions, allowing them to evolve over time – a crucial consideration, for instance, when dissecting the European RSC. However, these regions are not arbitrarily delineated. Buzan emphasizes that "RSCs define themselves as substructures of the international system by the relative intensity of security interdependence among a group of units, and security indifference between that set and surrounding units" (Buzan & Wæver, 2004, p. 48).

So, how does Buzan conceptualize a regional security complex (RSC)? At its core, an RSC is defined as "a set of units whose major processes of securitisation[1], desecuritisation, or both are so interlinked that their security problems cannot reasonably be analysed or resolved apart from one another" (Buzan & Wæver, 2004, p. 44). This definition unmistakably carries a constructivist undertone, acknowledging the somewhat constant nature of regions in the short run, but also recognizing the potential shifts in the units' composition over time. This sense of constancy is rooted in the understanding that processes of securitisation and desecuritisation are not conjured from thin air. More often than not, they leverage pre-existing realities, such as geographical closeness. Yet, the fluidity of RSCs is justified by the evolving relationships of friendship and hostility among units within a specific RSC over time.

The emergence of RSCs stems from the dynamic interplay between the inherent anarchy and its resulting balance-of-power implications, juxtaposed with the imperatives of geographical vicinity (Buzan & Wæver, 2004, p. 45). This unique interaction, set against a

[1] A term connected to the Copenhagen School, which designates a rhetorical process through which a problem is presented as an existential threat and thus justifies the taking of measures which would be outside normal political procedures (Buzan et al., 1998, pp. 23–26)

backdrop of geographical closeness, catalyses developments that mold the RSC. The units ensnared in this balance-of-power framework evolve to create intricate webs of alliances and rivalries. These "historical hatreds and friendships, as well as specific issues that trigger conflict or cooperation, take part in the formation of an overall constellation of fears, threats, and friendships that define an RSC" (Buzan & Wæver, 2004, p. 50).

Amidst their interactions, these units can inadvertently pave the way for external actors to influence or intervene in the region. However, such intervening actors are typically those with both the capability and stake, predominantly superpowers and global powers.

To dissect any given regional security complex (RSC), Buzan and Waever pinpoint four interconnected levels of analysis, which they term "the security constellation" (Buzan & Wæver, 2004, p. 51):

- *Internal Dynamics within States of the Region*: this level zeroes in on the threats or vulnerabilities experienced by states or groups of states within a specific region. For instance, a state's internal failure inherently ripples out, creating security concerns for its neighbors, regardless of whether it harbours aggressive intentions towards them.
- *State-to-State Relations*: this dimension captures the interactions, both collaborative and adversarial, between individual states within the RSC.
- *Engagement with Adjacent Regions*: this level recognizes that RSCs do not exist in isolation and focuses on their interactions and engagements with neighbouring regional complexes.
- *Influence of Global Powers*: this final layer acknowledges the often-significant impact and influence of global superpowers within the region, which can shape the RSC's dynamics and trajectories.

In addition to the aforementioned components, the concept of the "subcomplex" stands out. Serving as an intermediary stratum between individual states and the broader region, a subcomplex retains properties characteristic of an RSC. However, the defining feature of a subcomplex is that it is "firmly embedded in an RSC" (Buzan & Wæver, 2004, p. 51).

While traditional security apprehensions often focus on neighbouring states, in a security community, member states undergo a process of desecuritisation concerning their fellow members. However,

this does not imply a complete eradication of their security concerns simply by virtue of being part of a regional security community. Contrary to such a notion, the most evolved security communities today do not just dispense with security apprehensions. Instead, "the most mature cases of security communities today are not marked by a general forgetting of security concerns but rather by a conscious aggregation of them" (Buzan & Wæver, 2004, p. 57).

The near abroad as a potential Regional Security Complex

The "near-abroad" is a concept which has a deep symbolic meaning and implications. It is both about geography, and about symbolism, and is thus distinct from the general geographic vicinity. As a noun, "near-abroad" is a translation of the Russian *бли́жнее зарубе́жье* (romanized – *blizhneye zarubezhye*), a term whose origins and implications are far from established and certain. The original expression is a juxtaposition of the terms *бли́жнее* which has the meaning of "near" or "neighbour" and *зарубе́жье* which is a word composed through the combination of the noun *рубе́ж* which means "border" and the prefix за which translates as "beyond". It is not entirely clear as to how the term entered into use, Safire notes that "it was used firstly by Russians with a derogatory connotation, as indicating those areas at the periphery of the Soviet Union that, particularly towards the end of the Soviet Union, were seen as inflicting more costs on the budget of the Union than the benefits they provided" (*1994*).

The "near-abroad" would thus be comprised of the countries that are located in close geographical proximity to the Russian Federation. However, this definition, with its geographical undertones, would be inaccurate, as geographical proximity alone is not the criteria that unite the states comprising the "near-abroad". The term is more political than geographical, the uniting factor being their quality as states created by the dissolution of the Soviet Union. This title is used extensively in, and referring to, Russia and its interest, whereas the countries it aims to encompass do not recognize the validity of the designation. However, being a part of the Russian political identity, it determines the behaviour of this state towards the countries located in this geographical space. Thus, the main utility of the term is to distinguish between two different

types of foreign nations, the ones in the "near abroad" and all the others, located in varying proximity to Russia (proximity remains a relevant factor also regarding the other nations). In addition, not all countries in the "near-abroad" are considered the same in terms of their belonging to the "near-abroad", there are demonstratively different approaches to the Baltic countries, the Central Asians ones, and Ukraine or Belarus.

We could argue that the designation of a certain geographical space as "near abroad" is a speech act to refer to the terminology that the Copenhagen School borrowed from the philosophy of language. It does not only express information, but also performs the action of trying to shape perception both for the internal and the external public. It thus adds a trait to the Russian national identity, comprised of both Russians that inhabit its territory and those that inhabit its former territories, and it aims at stimulating a similar perception in neighbouring countries, which find themselves bound by ties that the dissolution of the USSR did not break. It is an attempt at continuation of the soviet common identity, as it was perceived by the Russians, centred on Russia, and with the other identities subservient, and not as equals. This designation has discursively justified a policy of dealing with the newly independent state not as fully-fledged sovereign nations „to be dealt with on an equal basis but as continuations, albeit under a new label, of the old union republics linked in different degrees of closeness (but never too loosely) to Mother Russia" (Rywkin, 2003).

The vicinity is part of the general impositions of geography that influences a state's behaviour in the international arena. All the states have a particular interest in their geographic adjacency, which represents most of the time the area where security interactions are significantly more frequent than outside this general area (Pop, 2016), and great powers are naturally sensitive about the interference of other powers in their vicinity. This certainly has been the case with NATO, and general Western institutions' expansion in the "near-abroad".

Because of the relative nature of the geographical factor together with the expanse of the Soviet Union, the "near-abroad" is far from homogenous. There are distinct geographical regions with different relations to the Russian Federation, and towards which this state has had varying goals, under the general objective to maintain some sort of

security buffer, and has employed several means to reach them, of which cyber-attacks are just one of the avatars facilitated by the technological development of societies.

We can thus distinguish between:

- **The Baltic States**: Estonia, Latvia, and Lithuania, have been constituents of the Russian Empire starting with the 18th century and, after a brief period of independence following the First World War, were annexed by the Soviet Union following the Ribbentrop-Molotov pact. They were some of the first to declare independence following the fall of the USSR, and have followed a constant policy associating themselves with the West, rejecting participation in the Community of Independent States (CIS). They are presently members of NATO and EU and thus firmly placed in the Western sphere of interest while having very vocal security concerns towards the Russian Federation. However, the Russian Federation still has significant leverages to pressure them, particularly in the economic sphere, where the energy infrastructure is still interconnected. Also, the number of ethnic Russians in these countries is approximately one million, and they form a significant minority particularly in Estonia (24% of the population) and Latvia (25% of the population).
- **Central Asia:** Kazakhstan, Kirgizstan, Turkmenistan, and Uzbekistan have become a part of the Russian Empire during its expansions of the 18th and 19th centuries, and have been the last to proclaim independence. They are commonly characterized by the existence of authoritarian regimes that have been established after the fall of the Soviet Union. They are members of CIS to varying degrees part of Russian-promoted international organizations. The Russian Federation has historically acted in order to keep them as part of its sphere of influence, minimize Western influence (but it encountered significantly lower pressure than in Europe), and preventing the spread of instability from Afghanistan (Dubnov, 2018). However, the area has become of interest to China, which promises significant investments as part of its Belt and Road Initiative, an evolution that could strain the Russian influence in these countries.
- **The Caucasus:** Azerbaijan, Armenia, Georgia have entered into the componence of the Russian Empire in the late 18th, early 19th

century, and have always been somewhat of a powder keg of Russia. The three states have very different approaches to Russia, varying from very close, bordering complete dependence from a security point of view in the case of Armenia, to a respectfully balanced approach towards Russia and other powers in the case of Azerbaijan, and to a hostility that has led to conflict in the case of Georgia (Mammadov & Garibov, 2018). Russia still considers the area relevant to its national security, being concerned mainly about Western infiltration in the area, and has proved that it is willing to use force to prevent this.

- **Eastern Europe:** Belarus, Moldova, and Ukraine comprise together the most complex and problematic region, as they are not only part of the particular sphere of interest that is the "near-abroad", but also of arguably more importance as being on the main historical invasion route into Russia by European powers, and thus they ensure the strategic depth that protects Moscow (slightly less so in the case of Moldova). Moldova is a country that has a large (in proportion to its population) Russian speaking minority, and, at the moment, also as a consequence of the war in Ukraine, is on an accelerated Western path. Transnistria, as a breakaway self-proclaimed republic recognized by no state, but supported by Russian, together with the presence (despite International Law and Moldovan official demands) of Russian troops in this territory significantly impairs any real move outside Russian orbit. On the other hand, political turmoil aside, the situation in the country is stable and so it does not occupy an important place in Russian security interest.

Belarus is a Russian speaking nation and has been under the rule of the Lukashenko regime since 1994. The country was placed from the beginning in the Russian sphere of influence, a fact that Belarus not only didn't dispute but has at times manifested more interest in a closer relationship with the Russian Federation than Russia was willing to offer. The two countries have formed a Union in name but not in nature, and presently there is no clear direction of this political project.

Ukraine has also pivoted between East and West, but, as a consequence of its history as a frontier region of many empires, has accumulated fault lines between various regions that were activated when the country was on the verge of placing itself to firmly on a pro-Western path. Ukraine has always had an uneasy relationship with its

Eastern neighbour with which it was connected by a myriad of dependencies, most important economically and socially/culturally. Russia considers Ukraine a strategically important area, geopolitically important, and whose full sovereignty is unacceptable. The space occupied by Ukraine is also the cradle of the Kievan Rus from whence Russia draws its roots, so its loss would be unacceptable for the Russian Federation from multiple points of view. Thus, it accepted the potential consequences for the annexation of its territory, and even for its invasion, which turned into a protracted, costly conflict for both sides.

Thus, the "near-abroad" is not a unitary regional security complex at present time, but is actually a complex region where Belarus, Ukraine and Moldova together with the Russian Federation are the main constituents. The Baltics have become part of the EU-Western RSC thus facing at the moment many of the cyber threats (mostly espionage related) which generally target NATO member states. The Caucasus and Central Asia continue to be of interest for the Russian Federation, and arguably still a part of the "near-abroad", but their importance at the moment for Russia is diminished as the war in Ukraine continues to absorb most of its resources. This dynamic is evident in the case of the recent conflict between Armenia and Azerbaijan over Nagorno-Karabakh, where Moscow's involvement was minimal in spite of the killing of Russian peace-keepers. These dynamics are also observable in cyberspace, where countries face similar, or distinct threats based on their belonging to a specific RSC.

Real space vs cyberspace - the behaviour of states in cyberspace

Cyberspace is a term that has entered common parlance, although there are real challenges to us being able to truly discern what it refers to. Indeed, even the person that is credited with the invention of the term, the science fiction author William Gibson, has described it as "evocative and essentially meaningless" (Neale, 2000). Although as the Internet has begun as a project aimed at maintaining the availability of communication for the US government in the aftermath of a nuclear attack and there has arguably always been an involvement of the US national security apparatus in shaping its workings, this communication medium has been considered as an open medium where security came secondary if it were

a consideration at all. This has recently changed and as Dunn Cavelty notes "the securitization of cyberspace is perhaps the most important force shaping global communications today" (2016).

One of the most defining and essential characteristics of cyberspace is its intangibility, which stands in stark contrast to the physicality of conventional spaces. However, the intangibility is not total. Cyberspace is man-made, and runs on man-made, physical infrastructure, which ultimately behaves the same as other physical infrastructures. Cyberspace's infrastructure, including data centres, cloud storage facilities, and undersea cables, and is far from neutral. Ownership, control, and access to this infrastructure can determine data flow, storage, and retrieval.

Cyberspace is also fundamentally interconnected as it is constituted of extensive networks and connections that facilitate the rapid flow of information across various platforms, devices, and borders. In cyberspace, interconnectedness goes beyond mere technological links; it is the intrinsic fabric that allows for extensive global communication and integration. This quality enables real-time interaction, collaboration, and data exchange between users, irrespective of geographical locations.

In the lexicon of modern cyber warfare and espionage, few terms have garnered as much attention, and at times, notoriety, as "Advanced Persistent Threats" or APTs. To understand the seismic shifts in the landscape of state-sponsored espionage in the 21st century, one must delve deep into the world of APTs, the motivations driving them, and the intricate webs of state and non-state actors that employ them.

APT is an abbreviation of the term Advanced Persistent Threat, coined to illuminate some of the main characteristics of this kind of sophisticated cyber actor:

- *Advanced* – refers to the high degree of sophistication of their tools and modus operandi, which are usually accessible to some organizations and states due to the cost and resources involved.
- *Persistent* – refers to the fact that the actors have (in most cases) a persistent interest regarding a certain target and will be able to sustain an attack until they achieve their objective, but also to the fact that most Computer Network Operations (bar some types of operations aimed at creating effects in the short term) are aimed at creating some

sort of persistent access in the victim infrastructure, whether for intelligence exfiltration or as a backdoor for future operations.

To build on previously mentioned issue, there is no commonly agreed taxonomy regarding the types of activities states conduct in cyberspace, and the characteristics of the domain make it such that there is just partial overlap with our previous experience regarding power projection in the physical space (Singer & Cole, 2020). To clarify this issue, we will adopt the model proposed by (Monte, 2015) to distinguish between types of Computer Network Operations (CNO):

- *Computer Network Exploitation* (CNE) – which encompasses all activities aimed at the exfiltration of data from networks, activities that are commonly referred to as cyber espionage.
- *Computer Network Attack* (CNA) – which refers to various activities aimed at some type of modification of the target network. It applies to the destruction, denial, degradation, or destruction of some kind of target, whether it belongs to the cyber domain or not (e.g., economic or politically relevant targets). Thus cyber-attacks can also be a form of "political signalling" (Nye, 2017).
- *Computer Network Defence* (CND) – which comprises activities aimed at the protection of the networks belonging to the defender.

The argument for a regional cybersecurity complex

When examining the intrinsic nature of cyberspace, the concept of a regional cybersecurity complex might initially appear paradoxical. One of the foundational attributes of cyberspace is its borderless environment, where geographical demarcations are rendered inconsequential. Unlike conventional territorial domains, cyberspace epitomizes a truly global expanse, transcending physical boundaries and national jurisdictions.

This universal characteristic of cyberspace engenders a unique security paradigm. In the traditional geopolitical arena, as previously mentioned, threats often manifest based on geographic proximity or historical animosities, but in cyberspace, threat actors can, with relatively equal ease, target entities across vast distances without the need for physical ingress. Such a capability fundamentally alters the threat landscape. Furthermore, the pervasive nature of cyber threats underscores the global magnitude of the challenge. Cybercriminals,

hacktivists, or state-sponsored entities can operate from virtually any location, targeting any nation irrespective of geographical, cultural, or political affinities. This omnipresence of threats means that nations cannot solely rely on regional alliances or strategies to secure their digital domains.

However, with the aforementioned caveats, there are certain regional dynamics in cybersecurity that make the case for thinking regionally about challenges and responses:

State-to-State Relations.

Just as physical regions might share common adversaries or challenges, states within a certain digital region face threats from the same cybercriminal groups or state-sponsored actors, and in the "near-abroad" by far the most significant cyber threat is posed by the Russian Federation.

The Russian Federation is widely regarded as one of the most capable actors in cyberspace, the National Cyber Power Index created by the Belfer Centre for Science and International Affairs of the Harvard Kennedy School placing it on the third position all around, and on the second position in destructive capabilities (Voo et al., 2022). This state is one of the first adopters of cyber power, enjoys multiple advantages - some historical, and some as a result of policies adopted –, and has shown great prowess in developing and utilizing cyber capabilities. The Russian Federation is credited with deploying the first "large-scale state-on-state computer network intrusion set in history", named MOONLIGHT MAZE (Rid & Buchanan, 2015)

As part of its growing assertiveness in international relations. Russia has used a wide combination of cyber instruments to:

- Obtain strategic and tactical advantages through cyber espionage.
- Undermine the cohesion of the societies of perceived adversaries by a combination of cyber intrusion and informational operations (e.g.: the use of social media by the Internet Research Agency during the US 2016 Presidential elections).
- Enhance military operations (e.g.: Georgia 2008, Ukraine).
- Ensure "information security" and, by extension, regime security (Dunn Cavelty, 2016).

The resurgence of Russian state power supported by the extra revenue from growing oil prices at the beginning of the 21st century has been accompanied by near-constant cyber operations that have targeted with predilection neighbouring countries. The extent it is willing to go to varies, but it certainly is willing to bet like it was the case with Ukraine. Also, if from a geopolitical point of view, the Baltic States are outside its sphere of influence, they are still of special interest. As part of its strategy for its neighbourhood centred on hard-power (Pop, 2016). Russia has used cyber capabilities both as a tool in itself for hard-power projection, but most times as a support for other types of capabilities.

Given the nature of the internet, Russia has always been able to project power in cyberspace globally, thus being in direct contact with strategic opponents and being able to employ a combination of the above-mentioned instruments to achieve its objectives. Public reporting by cybersecurity companies and governments have associated state-sponsored cyber-attack groups with the targeting and occasional compromise of a wide number of countries and organisations. Thus, the main APT groups that have been up until the present time attributed to Russia are:

- *APT28* (a.k.a. Fancy Bear) – publicly associated with the Military Intelligence Directorate (GRU) and involved in CNE campaigns against a variety of targets at the global level, gaining notoriety for the hacking of the US Democratic National Committee in 2016 (UK National Cyber Security Centre, 2018), but also having targets such as the Parliament of Germany in 2015 ("Germany Issues Arrest Warrant for Russian Suspect in Parliament Hack," 2020), French TV network TV5Monde in 2015 (Lichfield, 2015), the Organization for the Prohibition of Chemical Weapons (OPCW) (*Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW - News Item - Defensie.Nl*, 2018), and a series of doping-related international sports organizations (*US Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*, 2018).
- *APT29* (a.k.a. Cozy Bear) – publicly associated with either the Federal Security Service (FSB) or with the External Intelligence

Service (SVR), and reported to be involved mainly in CNE type attacks regarding targets of strategic, political interest: the DNC together with APT28 (Alperovitch, 2016), Foreign Affairs Ministries in at least three European countries (Faou et al., 2019) and as of December 2020 an impressive number of US governmental targets (Nakashima & Timberg, 2020).

- *Snake* (a.k.a. Turla or Venomous Bear) – associated with the FSB and constantly targeting diplomatic targets in Eastern Europe (Diplomats in Eastern Europe Bitten by a Turla Mosquito, 2018).
- *Gamaredon* (a.k.a. Primitive Bear) – has been associated by the Ukrainian SBU with FSB (Operation Armageddon – A Look at Russian State-Sponsored Cyber Espionage, 2015) and has been mostly targeting Ukraine related targets (Testa et al., 2020).
- *Sandworm* (a.k.a. Voodoo Bear) – named after the references to Frank Herbert's Dune series that were identified in the code of the malware. It has been associated mainly with the attacks against the Ukrainian power grid that cause an interruption of function (Lemay et al., 2018), the NotPetya Ransomware campaign in 2017, and the attack against the opening of the Winter Olympic Games in Pyeongchang in 2018 (Greenberg, 2019). It is also publicly associated with the GRU.

The most important characteristic that distinguishes the Russian behaviour in the near abroad from its general behaviour in cyber space is the willingness it manifests to use all types of operations, even CNA type attacks aimed at the disruption or destruction of some infrastructure, generally in support of some higher objective of placing political pressure or supporting the reach of some other objective. This willingness to deploy cyber capabilities that have such potentially destructive effects is a mark of both the high degree of trust regarding the effects and the possibility to contain the effects, but also of the interest for the states that comprise this region. This kind of manifest confidence also supports the assertion that the "near abroad" is not perceived as an area comprised of Westphalian sovereign states, but of political entities that have more or less liberty of action according to their

strength (here their defensive cyber capabilities) and the leverage the Russian Federation has on them. Certainly, being located in the "near-abroad" means that the probability of having to deal with a type of CNA is higher, as the only other such incidents to date have been in the Middle East and, with the exception of Stuxnet, less advanced in nature.

We also note that CNE type operations, or cyber espionage in common parlance, does not distinguish between targets in the "near-abroad" versus in the general global interest of Russia. This is to be expected from a state that has invested and relies as much on cyber capabilities for obtaining intelligence. On the other hand, it is likely that the area is placed higher in the target list and thus sees more of this type of operations. It may certainly appear so given the frequent mentioning of targets in the "near abroad" in public reporting on Russian cyber activity. However, this kind of metric is not without potential errors (maybe this is just what is reported and does not reflect reality as there are more attacks than are reported or there are more attacks directed elsewhere which are not reported) and this can be a further area of developing this research.

Internal cybersecurity dynamics within states of the region

States within a region often deploy analogous technologies, engage with a consistent pool of vendors, or might even be interconnected through shared physical infrastructures like electrical power lines or energy infrastructure. Consequently, a cyber-incident in one state – whether it is a vulnerability exploit or a direct attack – can have cascading effects on its neighbours. We have yet to see a CNA against critical infrastructure which affected neighbouring states (as this would be highly escalatory), but if we consider physical attacks, the energy interconnections between Moldova and Ukraine resulted in blackouts in both countries after a Russian missile strike ("Most Moldovan Power Supplies Restored after Russian Strikes on Ukraine," 2022). The potential for a similar regional outcome resulting from cyber-attacks is significant, as at the global level there are increasing concerns about malware pre-positioning in critical infrastructure, particularly connected to Russian state sponsored attackers (Canadian Centre for Cyber Security, 2023).

Eastern Europe is mentioned frequently as targeted by the various campaigns associated with the Russian APT ecosystem. However there is a significant difference between Moldova, which is a target of CNE and "information operations", a blend of CNOs and disinformation/ propaganda (CERT-EU, 2019), and Belarus – a sporadic target of mostly CNE, as it became on the Russia's closest allies- and Ukraine, which is the focus of multiple APT groups and a wide variety of operations.

Cybersecurity researchers have noted that Ukraine is in all accounts a cyber-testing ground, where Russia first deploys cyber capabilities and tests different potential courses of action (Greenberg, 2017). Since 2013 Ukraine has been one of, if not the main target of Russian Cyber Attacks (Cerulus 2019), so it offers many examples of both CNE and CNA, but also some operations in support of other military operations. One of the first observations we can make is that during the initial conflict with Ukraine and the occupation of the Crimean Peninsula, is that expensive cyber operation was not necessarily always the solution for obtaining objective in cyberspace. For example, during the occupation of Crimea one of the presumed objectives, obtaining control over the flow of information and blocking communications with the mainland, has been obtained simply by disrupting the Internet Exchange cables that assured the physical connection to Ukraine (Geers 2015). However here too the most relevant and concerning operations were those that aimed at producing some kind of physical effects. Three distinct operations fit this description: two directed against Ukrainian energy-producing and distribution networks (BlackEnergy in December 2015 and Industroyer in December 2016) and the most expensive and destructive ransomware to date-NotPetya, in June 2017. All three have been attributed by the US to the Sandworm group, and actually to specific officers inside the GRU ("FBI Deputy Director David Bowdich's Remarks at Press Conference Announcing Cyber-Related Indictment of Six Russian Intelligence Officers – FBI" 2020).

First in 2015 and then in 2016, in both cases during wintertime, the energy infrastructure in Ukraine has been targeted by malware that has been associated with Sandworm. The 2015 attack started on December 23rd and consisted basically of disconnecting energy substations belonging to three Ukrainian energy distribution companies, which caused a blackout for nearly 225.000 customers for more than

6hours (Greenberg 2019). In addition, given the deletion of some software components of SCADA systems, in some parts of the Ukrainian power sector, the attack meant the loss of automation for more than a year ("Crashoverride Analysis of the Threat to Electric Grid Operations" 2017). The 2016 attack also took place in December, on the 17th, and was an improvement in terms of the malware used and the objectives. Firstly, it was specifically designed to target transmission level substations in Ukraine and became the "second-ever specimen of code that directly attacked the physical world" (Greenberg 2019) after Stuxnet. As to its objectives, initial reporting ("Crashoverride Analysis of the Threat to Electric Grid Operations" 2017) suggested that its limited nature (targeting a single substation) and some characteristics of the internal code were proof that the attack was meant as a test, a "proof of concept" rather than a real cyber-attack. However, subsequent analysis (Greenberg 2019) suggests that the malware was meant to cause a second, permanent effect when the engineers tried to remedy the initial disruption. This second component appears to have failed.

The 2017 NotPetya ransomware campaign spread from a small company that offered and accounting software (M.E. Doc) in Ukraine to gain global visibility and impact. It affected systems belonging to the Ukrainian government (Health Ministry, various hospitals, the Post Office), the Chernobyl clean-up facility, the Danish Shipping company Maersk, the pharmaceutical company Merck, but also the state-owned company Rosneft, the steelmaker Evraz, the medical technology firm Invitro and Sberbank (Greenberg 2019). The attack caused 10 billion dollars in damages, and, unlike regular ransomware, it could not revert the damage (unencrypt the files). This fact, together with the fact that there was no way in which the attacker could communicate with the victims (the email address indicated was blocked by the email provider for breach of terms of service) made specialist assume that the attack was meant just to cause damage or destroy information (Goodin 2017). It likely was even more successful than the attackers assumed.

The war in Ukraine brought in its wake a wide array of cyber-attacks, most of them for cyber espionage, but also occasionally destructive in intent. The Ukrainian State Service of Special Communications and Information Protection currently tracks at least 23 groups which are considered to be Russia-led (State Service of Special Communication

and information Protection of Ukraine, 2023a, p. 12). In the context of the invasion, and to support the warfighting, destructive attacks have targeted a very wide array of industries and technologies such as the KA-SAT satellite network (Viasat, 2022), media, energy, logistic and telecom providers in Ukraine (State Service of Special Communication and information Protection of Ukraine, 2023b).

In the Baltic States, the main focus appears to be CNE type operations, aimed at exfiltrating intelligence, with CNA operations being rare but always a possibility. However, the best-known cyber-attack that took place in this region was the CNA type operation that targeted Estonia in 2007, and that made many governments wary of the disruptive and destructive potential of cyber operations. Thus, following tensions between the Estonian and Russian governments regarding the relocation in Tallinn of a statue of the Red Army soldier, the Estonian governmental, banking, and mass media infrastructure has been targeted by a *distributed denial-of-service* (DDoS)[2] type attack that paralyzed the country for the better part of two weeks. Some of the compromised websites also have been "defaced"[3], "replacing the content of websites with swastikas and pictures of the country's prime minister with a Hitler moustache, all in a coordinated effort to paint Estonians as anti-Russian fascists" (Greenberg, 2019). The attack has been attributed to Russian concern due to its interest in the matter, geopolitical reasons of state and the need for some kind of coordination, particularly to sustain the attacks, but as this kind of attacks that have a distributed infrastructure (multiple servers some belonging to civilians), the attribution is a weak one. It is to be noted that Vladimir Putin did make a veiled reference to the incident in his Victory Day speech, mentioning "those who desecrate monuments to the heroes of the war are insulting their own

[2] A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. See more on What Is a Distributed Denial-of-Service (DDoS) Attack?

[3] Web defacement is an attack in which malicious parties penetrate a website and replace content on the site with their own messages. The messages can convey a political or religious message, profanity or other inappropriate content that would embarrass website owners, or a notice that the website has been hacked by a specific hacker group. See more Imperva.

people (and) sowing discord and new distrust between states and people" (Faulconbridge, 2007).

The focus on CNE type operations is similar if we look at Central Asia, a report by Kaspersky ("A Slice of 2017 Sofacy Activity," 2018) indicating interest for a variety of targets (e.g.: science and engineering centres, Industrial and hydro chemical engineering and standards/ certification, ministries of foreign affairs, embassies and consulates, national security and intelligence agencies, press services, NGO – family and social service, ministry of energy and industry) located in all the nations component to the region. We have yet to have reported any CNA type operation in the area.

The countries of the Caucasus have mostly been targets of CNE operations that appear to be constant ("A Slice of 2017 Sofacy Activity," 2018) particularly aimed at discerning relations with NATO ("APT28 Delivers Zebrocy Malware Campaign Using NATO Theme as Lure," 2020). However, there is a distinction to be made between Armenia and Azerbaijan, who correspond firmly with this assertion, and Georgia, who has placed itself on antagonistic positions towards Moscow and has been involved in an open conflict with Russia.

The Russo-Georgian war of 2008 has been the first example of Russian use of CNOs in support of military operations. The modus operandi bears resemblance to what happened in Estonia in the previous year: a massive DDoS attack that accompanied the advance into Georgia by the Russian Army and that put out of work the websites of several central Georgian institutions (Ministry of Foreign Affairs, Presidency), the embassies of US and UK, but also those of the media and local institutions in conjunction with physical attacks against targets from different parts of the country (Greenberg, 2019). Georgia, due to its pro-Western orientation and weak cyber capability, is a recurring target of CNOs perpetrated by Russian APT's. In October 2020 the US authorities have indicted six GRU officers that are connected with the Sandworm group which they accused, among others, of "destructive, disruptive, or otherwise destabilizing computer intrusions and attacks (…) on Georgian Companies and Government Entities: a 2018 spear phishing campaign targeting a major media company, 2019 efforts to compromise the network of Parliament, and a wide-ranging website defacement campaign in 2019" (US Department of Justice, 2020).

Engagement with adjacent regions and global powers

The most important interaction in the region is that with the European Union, a normative superpower, and arguably a complex and multifaceted regional security complex on its own. The EU constitutes an institutionally centred RSC, up to the moment the security concerns of member states being dominated by their belonging to the EU. On the other hand, inside the EU RSC we can of late identify multiple sub complexes with individual, not always overlapping security concerns. Thus, the eastern periphery sees an existential threat in the resurge of Russia and the hard power instruments this state employs in its neighbourhood, a threat that is geographically distant and thus less relevant for the West or South of Europe. The South is confronted with migration and terrorism, having various failed states in its vicinity, a threat that indirectly affects the rest of Europe. The centre is in turn more preoccupied by political and economic evolutions inside the EU, trying to balance, and still maintain its control over the periphery and EU affairs, and at the same time dealing with migrant waves that aim for the economically prosperous areas.

Thus, European security continues to be marked by its perennial concern for societal evolutions but also has to balance a common response to threats that are not always felt with the same intensity. For the moment the RSC is stable, as the consequences of the changing the *status quo* are unpredictable, but arguably detrimental to European security. As more and more voices ask for internal changes, and reforms are needed in order to deal with security issues, it is expected that there will be an internal transformation, but the complexity of the RSC makes it exceedingly difficult to offer predictions on what those changes will look like.

From a cybersecurity point of view, the most important effects of the EU are in terms of regulatory influence, as EU member states and candidates adopt cybersecurity regulations like the NIS2 – Directive (EU) 2022/2555 –, aimed at boosting the overall level of cybersecurity in the EU (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) | Shaping Europe's Digital Future*, 2023). Of course, the regulations are applicable for the whole of the European Union, but they have the effect of enmeshing the EU members on the

Eastern Flank together with candidates outside the EU in a shared framework of cybersecurity policies, regulations, and norms.

The US involvement in Eastern Europe, both bilaterally and through NATO, has been characterized by a robust commitment to fortify the region's cybersecurity infrastructure and capabilities. Recognizing the evolving cyber threats that Eastern European nations face, particularly from state-sponsored actors and sophisticated cybercriminal groups, the US has embarked on a series of bilateral engagements, offering technical expertise, capacity-building programs, and information-sharing mechanisms to bolster regional cyber resilience. Concurrently, within the NATO framework, the U.S. has been instrumental in advancing the Alliance's cyber defence strategy. The establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, is a testament to this commitment, with the US playing a pivotal role in its operational success and strategic direction. Moreover, joint cyber exercises, like the annual "Locked Shields," not only underscore the collective resolve to counter cyber threats but also enhance interoperability and foster a unified cyber defence approach across the alliance. By intertwining its national strategic interests with the broader goals of NATO, the US underscores its dedication to a secure and resilient cyberspace for Eastern Europe, reinforcing the region's digital frontiers against potential adversaries.

Conclusion

The "near-abroad" is a symbolic, political rather than geographical space, a discursive construct aimed at shaping the Russian national identity and projecting influence in the ex-soviet states. The states that it refers to have as a major distinguishing characteristic their belonging to both a sphere of influence and a vital protection space, part of the strategic depth that ensures Moscow's protection. This kind of great power considerations trump the abstract principles of Westphalian sovereignty and justify interventions that could be considered a form of coercion to maintain the status quo in the region and prevent encirclement by the West.

The events in the physical space are anticipated and sometimes complemented/supported by an event in cyberspace, where Russia is one of the most capable and active players. All the neighbouring states

are a target of cyber espionage conducted by APT groups associated with Russian institutions. However, the fact that sets them apart is the probability of confronting some kind of cyber-attack aimed at disruption or destruction should their decisions be not to Moscow's liking. In this case, civilian infrastructure is both a valid and likely target. If we are to analyse the last twenty years, CNE is far more common than CNA, but there have been major incidents of attacks aimed at the disruption or destruction of infrastructure in Russia's near abroad which show that Russia is both a capable actor but more importantly one willing to employ these capabilities even when the effects are hard to anticipate (as in the case of NotPetya ransomware).

By conceptualizing cybersecurity at a regional level, policymakers can better anticipate shared threats, pool resources and expertise, and create more effective regional defense mechanisms against cyber adversaries. Moreover, understanding the interconnected nature of digital threats within a region can foster collaboration and trust among states, essential components in creating a robust collective cyber defence.

References:

1. *A Slice of 2017 Sofacy Activity*. (2018, February 20). https://securelist.com/a-slice-of-2017-sofacy-activity/83930/

2. Alperovitch, D. (2016, June 14). *Bears in the Midst: Intrusion into the Democratic National Committee*. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

3. *APT28 Delivers Zebrocy Malware Campaign Using NATO Theme as Lure*. (2020, September 22). https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/

4. Buzan, B., & Wæver, O. (2004). *Regions and Powers: The Structure of International Security*. Cambridge University Press.

5. Buzan, B., Wæver, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

6. Canadian Centre for Cyber Security. (2023, May 12). *The cyber threat to Canada's oil and gas sector*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector

7. CERT-EU. (2019). *Threat Landscape Report* (p. 4). CERT-EU. https://www.eui.eu/Documents/ServicesAdmin/ComputingService/Security/TLR2019Q1-Executive-v1.0.pdf

8. *Diplomats in Eastern Europe bitten by a Turla mosquito*. (2018). ESET. https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

9. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future*. (2023, September 27). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

10. Dubnov, A. (2018). Reflecting on a Quarter Century of Russia's Relations with Central Asia. *Carnegie Endowment for International Peace*, 13.

11. Dunn Cavelty, M. (2016). *Routledge Handbook of Security Studies* (2nd ed.). Routledge. https://doi.org/10.4324/9781315753393

12. Faou, M., Tartare, M., & Dupuy, T. (2019). *OPERATION GHOST – The Dukes aren't back – They never left* (ESET Research White Papers). ESET. https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

13. Faulconbridge, G. (2007, May 9). Putin jabs at Estonia at WW2 parade. *Reuters*. https://www.reuters.com/article/us-russia-putin-estonia-idUSL0957951620070509

14. Germany issues arrest warrant for Russian suspect in parliament hack: Newspaper. (2020, May 5). *Reuters*. https://www.reuters.com/article/us-russia-germany-warrant-idUSKBN22H0TB

15. Greenberg, A. (2017, June 20). How an Entire Nation Became Russia's Test Lab for Cyberwar. *Wired*. https://www.wired.com/story/russian-hackers-attack-ukraine/

16. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Knopf Doubleday Publishing Group.

17. Imperva. (n.d.). What is a Website Defacement Attack | Examples & Prevention | Imperva. *Imperva Learning Centre*. Retrieved May 19, 2024, from https://www.imperva.com/learn/application-security/website-defacement-attack/

18. Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

19. Lichfield, J. (2015, June 10). *TV5Monde hack: "Jihadist" cyber-attack on French TV station could have.* The Independent. https://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-french-tv-station-could-have-russian-link-10311213.html

20. Mammadov, F., & Garibov, A. (2018). South Caucasus as a Regional Security Complex: Divergence of Identity and Interdependence of Security. In *Cooperation in Eurasia: Linking identity, security, and development*.

21. Monte, M. (2015). *Network attacks & exploitation: A framework*. John Wiley & Sons, Inc.

22. *Most Moldovan power supplies restored after Russian strikes on Ukraine*. (2022, November 23). Reuters. https://www.reuters.com/world/europe/half-moldova-without-power-after-russian-strikes-ukraine-deputy-pm-2022-11-23/

23. Nakashima, E., & Timberg, C. (2020, December 14). Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce. *Washington Post*. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

24. Neale, M. (2000, October 4). *No Maps for These Territories* [Documentary]. Mark Neale Productions.

25. *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW - News item—Defensie.nl*. (2018, October 4). [Nieuwsbericht]. Ministerie van Defensie. https://doi.org/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw

26. Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44-71. https://doi.org/10.1162/ISEC_a_00266

27. *Operation Armageddon – A Look at Russian State-Sponsored Cyber Espionage* (p. 51). (2015). Lookingglass Cyber Threat Intelligence Group. https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf

28. Pop, A. (2016). From cooperation to confrontation: The impact of bilateral perceptions and interactions on the EU-Russia relations in the context of shared neighbourhood. *Eastern Journal of European Studies*, *7*(2), 24.

29. Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4-37. https://doi.org/10.1080/01402390.2014.977382

30. Rywkin, M. (2003). Russia and the Near Abroad Under Putin. *American Foreign Policy Interests*, *25*(1), 3–12. https://doi.org/10.1080/10803920301110

31. Safire, W. (1994, May 22). On Language. The Near Abroad – The New York Times. *The New York Times Magazine*, 16.

32. Singer, P., & Cole, A. (2020). *A Warning from Tomorrow*. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

33. State Service of Special Communication and information Protection of Ukraine. (2023a). *Russia's Cyber Tactics H1'2023* (p. 21). State Service of Special Communication and information Protection of Ukraine. https://cip.gov.ua/en/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit

34. State Service of Special Communication and information Protection of Ukraine. (2023b). *Russia's Cyber Tactics: Lessons Learned 2022* (p. 33). State Service of Special Communication and information Protection of Ukraine. https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine

35. Stewart-Ingersoll, R., & Frazier, D. (2012). *Regional Powers and Security Orders*. Routledge. https://doi.org/10.4324/9780203804995

36. Testa, D., Martire, L., & Pirozzi, A. (2020, February 17). Cyberwarfare: A deep dive into the latest Gamaredon Espionage Campaign. *Yoroi*. https://yoroi.company/research/cyberwarfare-a-deep-dive-into-the-latest-gamaredon-espionage-campaign/

37. UK National Cyber Security Centre. (2018, October 3). *Reckless campaign of cyber-attacks by Russian military intelligence service exposed*. Www.Ncsc.Gov.Uk. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

38. *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*. (2018, October 4). https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

39. US Department of Justice. (2020, October 19). *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. Www.Justice.Gov. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

40. Viasat. (2022, March 30). *KA-SAT Network cyber-attack overview*. Viasat.Com. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

41. Voo, J., Hemani, I., & Cassidy, D. (2022). National Cyber Power Index 2022. *Cyber Power*.

42. *What is a distributed denial-of-service (DDoS) attack?* (n.d.). Cloudflare. Retrieved May 19, 2024, from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

43. Wunderlich, J.-U. (2016). *Regionalism, Globalisation and International Order: Europe and Southeast Asia*. Routledge. https://doi.org/10.4324/9781315604459