IMSISS
International Master
Security, Intelligence
& Strategic Studies

Erasmus
Mundus

Cyberattacks: A New Weapon in The Economic Warfare Toolkit?

A Study of Russian Cyberattacks on the European Energy Sector in 2022

August 2023

University of Glasgow: 2704155m
Dublin City University: 21109494
Charles University: 15534539

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word count: 25,284
Supervisor: prof. Vit Stritecky
Date of Submission: 20-08-2023

University of Glasgow
DCU
CHARLES UNIVERSITY

TABLE OF CONTENTS

1. INTRODUCTION

In the days leading up to Russia's invasion of Ukraine on February 24, 2022, external observers expected cyberattacks to play an important role in the conflict. In March, newspapers were filled with warnings about the potentially fatal consequences of cyberattacks targeting critical infrastructure in the context of the Russo-Ukrainian war, and the possibility of these —with ominous mentions to cyberwar— affecting many other Western nations. The U.S. president warned the private sector of a possible spike in cyberattacks from Russia in retaliation for the penalties imposed on the country, interpreted by some as an attempt to raise awareness of Russia's capabilities and playbook –if not more literally.

However, reality fell short of meeting said expectations. But the fact that Russian cyberattacks underperformed estimations does not imply that they do not pose a threat in the current geopolitical landscape, particularly for European countries which have demonstrated their support for Ukraine and distanced themselves from Russia. These may be less attention-grabbing and spectacular than other types of (kinetic) attacks, but they characterise the bulk of incidents faced by companies and institutions globally day-to-day, and contribute to the overarching destabilisation of the targets. This dissertation will not attempt to prove the decisiveness or effectiveness of cyberattacks as a form of economic coercion in the context of a war, but rather prove that this is a phenomenon worthy of consideration and theorisation.

1.1Aims and Objectives

Principally, this dissertation seeks to answer the question of whether cyberattacks serve as a new coercive tool in contemporary economic statecraft. Beyond this practical objective, the research conducted throughout hopes to:

- Shed light on the potential use of cyberattacks as a coercive tool in the realm of geoeconomics and economic warfare, and address and fill a critical vacuum in academia regarding this nexus;
- Highlight the strategic nature of these attacks that fall short of the threshold of physical damage and explore a new approach to state aggression;
- Attribute the necessary importance to the cumulative impact of cyberattacks associated with nation-states which target key sectors of their rival's economy;
- Identify patterns between attacks to elevate them from the category of crime to that of "warfare";
- Illustrate the close links between private entities and nation-states and their impact on geopolitical dynamics;
- Contextualise the cyber-economic weapon within Russia's toolkit vis-à-vis Europe.

1.2 Research Design and Methodology

The focus of this dissertation revolves around an intricate and comprehensive exploration of cyberattacks that have been directly or indirectly attributed to Russia and specifically targeted the energy sector throughout the year 2022. At the heart of this study lies a crucial research question: "Can cyberattacks serve as a potent geoeconomic instrument and an effective tool of economic warfare in the hands of Russia?"

This inquiry takes on heightened significance within the broader context of the tumultuous relations between Europe and Russia, notably exacerbated by the ongoing conflict between Russia and Ukraine. Against this backdrop, the dissertation embarks on a comprehensive investigation, meticulously examining key aspects that demarcate a cyber operation or attack as a potential manifestation of cyber-economic warfare. This will be materialised in the form of a single (qualitative) case study, applying different methodologies conducive to various layers in the argumentation and taking a deductive approach. Such a design will also be valuable for the purpose of triangulation. Following a qualitative approach allows the bridging of limitations in the availability of certain numerical data and establishes a pattern in the type and scope of various cyberattacks, the profile of the targets, the alleged attackers (justifying their link to Russia as a nation-state), and most importantly, their ulterior motive. The research will be limited to the energy sector as a target given its significant role in the economic stability of a country and its centrality in Russian-European relations.

The case study will be further supported by a series of sections devoted to the contextualisation of the prevailing state of affairs in Europe during 2022 and the wider relationship between Russia as a state and its hackers. More specifically, it will look at the geopolitical landscape in 2022 influenced by the war in Ukraine, how this has affected the relations between Russia and other European countries, and the role of energy in said relations before and during the conflict. It will additionally include a brief description of the unfolding of the energy crisis in 2022, as the aforementioned cyberattacks did not take place in a vacuum. Moreover, this dissertation further observes the existence of a precedent of cyber-economic warfare within Russia's strategic playbook and describes the connections between the Russian state and an array of hacking groups, unravelling the symbiotic relationship that enhances the state's plausible deniability and capitalises on the intricate challenges of cyber attribution.

By shining a light on all these relationships, the study attempts to provide readers with a more complete understanding of the motivations and entities driving cyber-economic warfare.

The analysis comes into being through a curated collection of 40 cyberattacks that targeted the energy sector in 2022, all in some manner associated with Russia. The criteria employed to delineate these cyberattacks as instances of cyber-economic warfare is multifaceted and derived from the theoretical framework. It seeks to include various theories offered by scholars and researchers since the 1990s until our days, merging reflections on economic warfare and economic coercion with literature on cyberwarfare. Thus, this dissertation first probes whether these cyberattacks are part of larger strategic operations or standalone events. Second, it investigates the potential geopolitical motivations that underpin these cyber incursions. Third, it examines the linkages between the perpetrators and a nation-state, with Russia as a central focus —integral to this assessment is the question of whether these actors are sponsored or endorsed by the Russian government, they actively support its policies abroad taking upon themselves the mission to represent it, or their goals simply align. Fourth, it seeks to ascertain if these attacks bear on crucial economic targets and whether these operations intend to exert an economic impact on the targeted entities. To a lower extent, the analysis considers whether these attacks could be construed as potential military targets and attempts to estimate the extent of the damage (mainly the economic cost) inflicted by these types of attacks. Fifth, this dissertation explores whether these attacks could constitute instances of coercion—signifying a concerted effort to exert pressure on the targeted entities to effect policy changes, demanding compellence or as a deterrent—or if they signal disapproval or dissent. By methodically applying this comprehensive framework, the dissertation endeavours to illuminate the intricate interplay between cyberattacks, economic warfare, and geopolitical dynamics in the specific case of Russia's energy sector targeting in 2022.

Limitations

A potential issue that the author will strive to bear in mind is that through focusing on a single case study, any conclusions subsequently drawn from the findings could be considered temporal, non-generalisable, and subjective in nature. Nevertheless, this can often be said about qualitative research as a whole.

Furthermore, it would be extremely hard to isolate the extent of the damage caused to the wider economy of the countries at hand from other economic variables. Moreover, delays in the disclosure of information regarding cyber incidents are common, while public information regarding the cost for the affected parties is limited. Extensive research demonstrates the difficulty to quantify the exact effects stemming from the use of any kind of coercive economic instrument as well as their efficacy. Accordingly, the dissertation will not seek to answer the question of whether these instruments "actually work". Cyberattacks are understood as a supplementary element (one of many instruments) within a broader strategy, aiming to exert economic pressure on Russia's adversaries to improve its geopolitical standing and limit support to Ukraine. The assumption is, however, that the indirect impact of cyberattacks is greater (or goes beyond) the immediate associated direct costs to the target.

At the same time, the timeliness of this research presents other limitations. The fact that the conflict studied is currently still developing implies a certain level of uncertainty regarding Russia's actions. We cannot assess with complete confidence that cyberattacks on the energy sector will continue taking place at the same rhythm and will be limited to the same magnitude. Until the conflict is over, it is unlikely that we will be able to gain a comprehensive understanding of the cyber aspect of Russian strategy in the war, particularly when this extends beyond Ukraine. Likewise, as it will be explored throughout the dissertation, the attribution of cyberattacks remains a complex task. On top of this, researchers face the challenge of monitoring the perpetrators –often morphing into new organisations– and demonstrating their connection to a nation-state (attribution).

1.3 Literature Review

The theoretical framework supporting this thesis is primarily underpinned by the framing of geoeconomics as outlined by Blackwill and Harris, alongside the wider body of research on economic coercion (2016). Blackwill and Harris define geoeconomics as "the use of [economic] instruments to promote and defend national interests, and to produce beneficial geopolitical results" thus affecting the stability of the adversary. Cyberattacks are considered in their book to be one of seven economic instruments. However, Blackwill and Harris consider the "cyber-sphere" and "energy and commodities" as two instruments existing in parallel on the same level, while this dissertation will rather favour the instrumentalisation of cyberattacks and the energy sector as a target. The book does not properly address either of them, as it focuses instead on the use of economic instruments as a whole in the United States. Despite this, compared to traditional models of geopolitics, this framework provides an underexplored and interesting approach to understanding state aggression in the present time. In their own words, "geoeconomics stands as both a method of analysis and a form of statecraft [...][whereby] a state builds and exercises power by reference to economic factors rather than geographic ones" (Blackwill and Harris, 2016).

The greater body of academic research today available frequently hyper-focuses on hybrid warfare and cyberwarfare - repeated to the point of being stale or commonplace - in lieu of economic warfare. Such a conceptualisation has also been adopted by major international organisations and alliances like NATO, which considers cyberattacks as a form of hybrid threat (2023). Moreover, the conflict between Russia and Ukraine is systematically referred to by the international community as a model case of hybrid warfare. The trendy concept of hybrid warfare, with its endless list of definitions, acts as an umbrella term for anything outside the realm of what is strictly "military" and involves any actor beyond the state. While not often rendered to criticism, this 'buzzword' is seen by some scholars as a mere rebranding or amalgamation of various existing concepts (Caliskan, 2016). This is apparent when listing all the actions supposedly available to a hybrid actor: economic disruption, cyber operations, the weaponisation of information, social/psychological manipulation, and the use of irregular and regular military forces alike (Abdyraeva, 2020).

Cyberwarfare is often seen as a subcomponent or domain of hybrid warfare. According to Ducaru, this connection is evident in Russia's deliberate combination of multiple instruments of power (including cyberwarfare) in a synchronised manner, which are blended together in Russian military doctrine (2016). Accounts or references to Russia's cyberwarfare campaigns in the year 2022 remain predominantly focused on Ukraine (where there is already a conflict underway in the most traditional way), with little to no mention of any other countries aside from potential spillover effects. The use of the term cyberwarfare becomes therefore confusing as, while theoretically broad, is often applied to contexts with traditional, kinetic elements. Moreover, it is not entirely unusual to find economic disruption as a type of cyberwarfare attack. The ambiguity and loose application of these labels makes research about the multifaceted phenomenon of cyberattacks a daunting task, at the same time that it invites the study of new approaches.

This dissertation attempts to itself apart from the pre-existing academic literature by addressing a critical vacuum - few, if any, publications exist which combine and analyze economic warfare, economic coercion, and cyberattacks, from a strategic point of view. The research is enriched by the timeliness and topical nature of its case study, due to the ongoing geopolitical climate in Europe, triggered by the Russo-Ukrainian war. Furthermore, it examines the overarching motives and logic of those behind non-physically damaging cyberattacks, aiming to contribute to our understanding of Russia without echoing the panic spread by a myriad of media articles about Russia's cyber potential for harm.

A discussion on economic coercion will constitute a substantive segment of the dissertation. As there is no academic theory on cyber-economic coercion, this research will draw upon publications in related and parallel fields of study, e.g. sanctions. An example of this is the research of Kimberly A. Elliott, which separates sanctions into three broad and overlapping categories: those that signal disapproval, those that coerce, and those directed at denying or containing something (2010). This categorisation of economic instruments based on the intent behind them will be applied to cyberattacks: are they a form of coercion or are they meant as a form of communication (of disapproval) in international politics?

Another interesting debate that has ramifications for the research is the one generated around the definition of cyberattack. It is unclear what we mean by cyberattacks, and what they entail nowadays. Although applicable definitions have been put forward by researchers including Owens et al. (2009) and Roscini (2014), perhaps the most advantageous for this research is one offered by Hathaway et al. (2012), due to its generality and openness. As this is likely to be of little practical use when it comes to the instrumentalisation of research by policymakers, we will rely on those definitions already operationalised, for example as presented by the NIST Computer Security Resource Center. The same lack of consensus and clarity characterises discussions around cyber warfare.

Economic warfare is a similarly difficult concept to apply to the research proposed, as it is fraught with dated and limited definitions. When cyberattacks are included in these discussions, it is only marginally. Current debates about economic warfare mainly call for its regulation, given its devastating impact in a globalised world. The Russo-Ukrainian war has also reignited debates about economic warfare, although they often place Russia on the receiving end of these instruments (mainly sanctions). However, if Russia is presented as playing an active role (as compared to being a passive recipient), cyberattacks are certainly not included in this context - with cutting gas supplies often emphasised instead. Likewise, media publications tend to equate financial warfare with economic warfare. Paul Bracken has problematised this situation and emphasises the importance of differentiating between financial warfare and classic economic warfare (2007).[1]

As mentioned above, there is a critical lack of convergence in these realms. There are three limited exceptions to this rule.

In the first place, we can find the research conducted by the Foundation for Defense of Democracies under the label of Cyber-enabled economic warfare (CEEW). They understand CEEW as a "concerted effort to target the pillars of a state's economy to undermine its ability to defend its citizens and project power abroad" (Ravich and Fixler, 2022). However, this description fails to adequately incorporate the cyber aspect. The Foundation emphasises that while CEEW was mentioned in the 2017 National Security Strategy published by the White House, the connection between malicious cyber-

[1] According to him "the economic system deals with the hard and soft outputs of the economy—that is, goods and services", while the financial system by contrast "deals with money and credit"

activities and wider strategies of states remains unclear. Unfortunately, this term is barely used in Europe (Ravich and Fixler, 2017).

A second exception is the research of Shmuel Even, who approaches the relationship between Economic warfare and the cyber realm to some extent (2018). In his paper on "Broad Economic Warfare in the Cyber Era", he suggests that cyber capabilities can be employed to damage an adversary's economy both during wartime and between wars (interpreted as peacetime). His analysis divides these efforts into defensive and offensive. The relevance of this bifurcation is limited for this dissertation given the narrative upheld by Russia regarding the West and Ukraine. In his "standard" definition of economic warfare, he does not seem to explicitly consider cyberattacks but they could perhaps be considered under "boycott to various economic areas". More interestingly, he offers a broader understanding of economic warfare, comprising different forms of cyber actions that he divides into "hard" and "soft" warfare. This dissertation would focus on the latter, where high-intensity attacks are not necessarily expected but rather "softer" cyber warfare. The dissertation would seek to expand upon this characterisation of "softer" cyber warfare within a broader understanding of economic warfare but referring to attacks other than "large-scale theft of intellectual property".

A third exception to the rule is Paul Cornish, who sets out to establish the composite idea of economic cyber warfare (2011). Regrettably, the article arguably fails to fully develop the concept, instead dwelling on establishing multiple parallels between cyber warfare and economic warfare. Moreover, his examples of economic cyber warfare focus on espionage or intellectual property theft, remaining relatively short-sighted. However, Cornish does contend that "economy might be the way, and cyberspace the means" through which a state can have its organisation disrupted, highlighting the "strategic end" and refusing to understand the motivation of cyberattacks as merely financial - a perspective aligned with the argument of this dissertation.

2. THEORETICAL FRAMEWORK

2.1 Geoeconomics, economic coercion, and economic warfare

In an increasingly interconnected world, the dynamics of international relations and economic interactions have undergone significant transformations. While traditional geopolitical analyses primarily focused on the role of military power and political influence in shaping global affairs, economic instruments —initially overshadowed— have become increasingly significant as their potential to exert influence, gain leverage, and advance (or safeguard) national interests (Blackwill & Harris, 2016) become evident to states worldwide. Far from resorting by default to the use of their military resources and toolkit, countries are utilising their economic power to shape both regional and global geopolitical outcomes, foster alliances, and engage in strategic competition. The use of economic power can be a more subtle means of pursuing geostrategic goals than displaying military might, with less risk of costly counter-reactions (Wigell, 2016).

The term 'geoeconomics', which emerged after the Cold War as one of the key conceptual frameworks —or "ideational constructs"— explaining international politics, (Kalyanaraman, 2017) was first coined in 1990 by Edward Luttwark in his essay "From Geopolitics to Geo-Economics" (Troxell, 2018). It challenged the notion of military power's predominant role in interactions between core states within the international system. Instead, it proposed that inter-state conflicts would largely revolve around economic considerations, moving from power projection through a military lens to "economics as the continuation of war by other means" (Daniel Bell). The Cold War rhetoric lost its raison d'être and a military confrontation between the Soviet Union and the West seemed less and less likely. As a result, the beginning of the 21st (and end of the 20th) century saw researchers announcing, in the style of Nostradamus, the end of history, and the triumph of liberalism as a political and economic model.

Geoeconomics is experiencing a resurgence today, while comparisons with other instruments of statecraft –diplomacy, military force, and information (Troxell, 2018)— have not been left behind. As the premise of the progressive loss of relevance of military power remains challenged by current events, particularly for Europe, it might be time to shift our perspective away from the substitution theory and recognise that military might and developments in the diplomatic sphere will go hand in hand with international economics. According to Luttwark, the logic of conflict which he describes as "adversarial, zero-sum and paradoxical" would remain intertwined with states' geoeconomic impulses, even if previously overshadowed by other strategic (security) priorities (Luttwark, 1990). He describes a world where we cannot establish a single superior modality (Luttwark, 1990). Economic and security considerations are certainly coming together in our days, but it would be erroneous to think that the proposal of a relationship between geoeconomics, diplomacy, and military efforts is as fresh in Blackwill and Harris' publications as some seem to think.

What was not presented as clearly in Luttwark's writings was the difference between geoeconomics and commerce —or trade—, frequently equated. The term has become quite popular, appearing in a portion of articles analysing US-China economic rivalry, but scholars cannot agree on one definition. However, the active use of economic instruments or interventions goes beyond limits to trade and investment. Wigell (2016) also denounces the use of geoeconomics as the commercial tactics of countries or economic geography, arguing that zero-sum interests do not fit within the logic of commerce, and would likely contravene a priori the establishment of mutually beneficial trade relations.

This coexistence of economic and security policies (inevitably influenced by geopolitical considerations and national interests, albeit not always exclusively centred on power projection) does not come without its problems or challenges. According to experts, the European Union is in a particularly difficult position when it comes to geoeconomics, given that it was originally built from the idea that economics and security should be separated (Wigell et al., 2022). It is believed that this circumstance has left it unprepared to deal with the growing convergence of these two realms and, overall, three major geoeconomic risks: geoeconomic dependence (involving the securitisation of the economy), geoeconomic disruption (or the weaponisation of the economy), and geoeconomic competition (leading to the balkanisation of the economy) (Wigell et al., 2022). This essay will focus on the first two risks, with particular attention to the second one.

The aforementioned geopolitical risks —risks connected to the use of economics by states for "power political objectives" (Fjäder et al., 2021)— appear to be a result of multiple phenomena. These include the 'securitisation' of the economy, states' focus on safeguarding strategic assets and infrastructure, and the privatisation of critical functions within the economy and society at large (Wigell et al., 2022). They also reflect international tensions and trends. According to Josep Borrell, EU High Representative, "economic interdependence is becoming politically very conflictual" (Borrell, 2020) (Wigell et al., 2022), as all the expectations projected on globalisation —a multipolar world with interdependencies deterring states from coercive measures— have not necessarily met reality. Often to the contrary, asymmetric dependencies resulting from integration have been exploited and leveraged, threatening states' strategic autonomy. Scholars like Joseph Nye asserted that leveraging asymmetries is a crucial feature of economic power (Nye, 2011). In the case of the EU, The European Parliamentary Research Service has also warned against the EU losing agency (autonomy), fearing that it will become a "playground for global powers" (Anghel et al., 2020) unless it learns to use both 'soft' and 'hard' power.

Moreover, securing critical infrastructure, from the perspective of the state (or even a regional organisation), is an ongoing and strenuous effort as these are operated, owned, and reliant on entities belonging to the private sector. Businesses, in turn, depend on global markets and supply chains (Fjäder, 2018). The threat of disruption then becomes a particularly effective coercive practice in an interdependent world. The EU's open market —the pillar of its existence— appears particularly vulnerable to economic coercion, while scholars also point out the downsides of lacking more centralised decision-making structures (compared to actors like Russia or China) (Wigell et al., 2022): it is not only hard to protect all entities within its borders, but also to respond decisively to disruptions in a timely manner. Adversaries can equally exploit the EU's structure and differences between its members, creating divisions by targeting countries asymmetrically.

All these actions could fall under the umbrella of 'economic warfare', but countries, particularly in Europe, tend to avoid this term. On the one hand, it might seem needlessly bellicose and offensive to modern Western pacifist sensibilities. On the other, much like with 'geoeconomics', the concept of economic warfare is lacking in clarity despite adding a dramatic flair to many articles. Across publications, the most resourceful definition of 'economic warfare' seems to be the one given by the Encyclopaedia Britannica: "the use of, or the threat to use, economic means against a country to weaken its economy and thereby reduce its political-military power." In a similar vein, it can be aimed at compelling an adversary to modify its behaviour or policies, or influence its relations with other countries (Shambaugh, 2022).

Building upon said definition, this dissertation will seek to provide a relatively comprehensive understanding of what economic warfare is and what it entails.

Each author has focused intently on a specific element or factor that epitomises economic warfare with the same purpose: shedding light on this type of warfare. Many focus on the different methods to weaken the adversary, adding to the extensive list of economic warfare techniques, whereas others centre their analysis on the objectives of such actions. This is further complicated by the history of economic warfare itself. Economic aggression was practiced already in Ancient Greece, and, as societies progressed or clashed, its tactics evolved (Ravich, 2015). Until the 20th century, states particularly resorted to this option in times of military conflict, where it played a significant but secondary role. Scholars also recognise that traditional forms of economic warfare were directed at objectives that likely differ from our current goals (Bogdanova, 2022).

Some of the most common forms of economic warfare include trade embargoes, blacklists, blockades, sanctions tariff discrimination, freezing of capital assets, counterfeiting, suspension of aid, restrictions on investment and capital flows, expropriation, preclusive purchase of scarce critical resources, manipulation of prices for critical goods, technology theft, or the disruption and sabotage of economic targets (Ravich, 2015). As indicated by the list above, the number of techniques is inclusive and ever-expanding. This dissertation will focus throughout the different chapters on the last one of those options. Furthermore, it will seek to add new tactics involving an alternative field. However, there are several issues associated with this general categorisation of actions and the lack of uniform criteria.

One of these problems is that, while economic warfare encompasses a wide array of economic, legal, and administrative measures directed at undermining the opponent's economy, it is still unclear when economic actions cross the line from being hostile to outright economic warfare (Slukhai, 2019). Shulsky proposes in this scenario a series of considerations that could contextualise and help understand the dimensions of the economic 'actions' (2015). He believes it might be relevant to bear in mind the degree of the state's involvement in the economy, its grand strategy —"to what extent does the country see itself as engaged in a zero-sum competition with its adversaries?", "does it see the weakening of an adversary as a necessary component of its future success?"— and the state's disposition or stance vis-à-vis international law or norms. These and similar inquiries can prove useful as a framework from which economic actions can be assessed and determine whether they belong to a broader campaign of economic warfare. Nevertheless, it is unclear with what degree of certainty a state could rely on these assumptions, as the answer can be influenced by biases like mirroring[2]. Shulsky himself admits this, adding to his analysis that further investigation of the "overall strategy" is necessary and that this area remains "quite speculative" (2015). Slukhai also adds another important element to this debate: some economic warfare actions, which could be indirect measures, are in fact "a by-product of other hybrid actions" (2018).

Other scholars, as commented above, place more emphasis on the result and what these economic actions are aimed towards. For example, Deakin considers economic warfare measures aimed at affecting trade conditions, market liquidity, denying market access, degrading market efficiency, degrading supply chains, and exploiting, denying or degrading supporting infrastructure or economic information (2003). For Shulsky, economic warfare serves three main purposes: a) diminishing the military and political power of an adversary, b) creating or worsening domestic political challenges for the adversary's government, with the goal of influencing policy changes or behavioural shifts, or c) instigating enough popular dissatisfaction to prompt the overthrow of a regime (2015).

[2] A type of cognitive bias that leads individuals to project their own beliefs or perspectives onto others and assume that they act or think in the same manner. In this case, it refers to a state assuming that another state would respond to a specific situation in the same way they would react.

These objectives are not too far, however, from the traditional understanding of economic warfare. Lambert also emphasises how economic warfare throughout history, has been focused on the enemy's society as opposed to the state (2017). He compares different forms of economic attacks, which he identifies with the First and Second World Wars: a war of attrition "designed to degrade the economy and a nation's warfighting capacity", and a war that is designed to impact the societal psychology. In his analysis, putting at the centre Great Britain's strategy in 1914, "the target was the systems supporting the society's lifestyle" to swiftly erode the domestic support for, legitimacy of, and confidence in the government. Yet the figures behind this reconceptualisation of war, struggled with transforming the theory into a feasible strategy and garnering a receptive audience at a time when, for economic warfare to work, it had to be approached as a national strategy (Lambert, 2017).

Today, scholars disagree on in which occasions economic actions can be classified as economic warfare and whether there is any difference between their use in peacetime, i.e. in the absence of a 'proper' war, and their employment during "violent conflict" (Shulsky, 2015) (Ravich, 2015). Furthermore, Slukhai identifies another obstacle, citing a publication by the Ukrainian National Institute of Strategic Studies: "Establishing a fact of aggression in the non-military spheres of social life is extremely complicated, or even impossible" (2018). Thus, we are forced to look back at the question of the ulterior motive: what is the primary goal of debilitating an adversary's economy? As previously stated, it is important to distinguish economic warfare from efforts to gain primarily economic advantages. This is why, despite the prevalence of zero-sum thinking among analysts, Slukhai seems to believe that economic warfare has more potential to be doomed and become a "loss/loss game" (2018).

Drawing from the general literature on Economic Warfare —which is regrettably all too often limited to sanctions—, measures are often categorised into the following groups depending on the ambitions of the "sender": those which intend to coerce, those that serve as a form of signalling, and those whose mission is to constrain.

The theory of coercion was developed by Schelling as a means of "hurting" an adversary while retaining or maximising the state's (the sender) bargaining power (1966). Coercive diplomacy does not necessarily require lethality or physical violence: it just needs to to inflict enough suffering to inspire the adversary to change a specific course of action (Steiner, 2016). This is achieved in two ways: "deterrence" and "compellence". Deterrence refers to the use of threats (or actions) to prevent the enemy from pursuing a certain policy or strategy (instilling fear in the consequences), while compellence emphasises the need for the adversary to undertake a particular action by balancing incentives and disincentives (Schaub, 2004). While the differences between the two are subtle and therefore difficult to identify, Schelling describes deterrence as an indefinite situation, passive, as opposed to compellence. Compellence must convey a deadline, involving questions of "where, what and how much" (Schelling, 1966). But there are alternative questions. Practitioners and researchers alike often refer to one other goal of economic warfare: "to constrain". However, in their definitions of this term, we can find similarities with the use of deterrence in the work of Schelling. One researcher, for instance, writes that "'constrain' seeks to prevent the […] state or entity from pursuing its course of action" through various means, as opposed to coercion which "imposes costs on the sanctioned state or entity to build up leverage for negotiations" (Rapnouil, 2017). He additionally advises that studies of economic measures' effectiveness should always refer to one of these aims.

While first approaches to researching economic coercion centred on its effectiveness —a subject that regains traction with every new iteration of sanctions—, scholars have only recently expanded their investigations to include the motivation behind states' use of economic coercion as well as the selection of specific coercive tools (McLean, 2021). In McLean's analysis, the main premise behind the coercer's actions would be to reduce the target's expected benefits from pursuing the policy they wish to avoid, thereby influencing the target to align its actions with the coercer's preferences and its success relies on the coercer's ability to impose costs on the opponent. In her publication, she narrows down economic coercion to negative economic measures and establishes a guiding path for those studying state behaviour. Said behaviour is influenced by three main decisions: target, the type of coercive instrument necessary to meet the goal, and the required "scale of coercive effort" (McLean, 2021).

Nonetheless, coercion is far from simple: it is neither a straightforward strategy nor a precise formula (Biddle, 2020). States' behaviour, and the effectiveness of economic coercion at large, rely on the perception of a significant danger or impact —of vulnerability— which would compel the targeted nation to take measures to avoid (further) harm. However, these "pressure points," which are deeply political and psychological, are likely to differ from one country to another (Steiner, 2016). According to Steiner, it is this subjective sense of vulnerability that matters more than the actual exposure (2016). Adding another layer of complexity, Byman and Waxman argue that coercive diplomacy should not be seen as a one-time event, but rather a series of moves and countermoves in an ongoing dynamic process between conflicting parties (2002). For researchers, isolation is difficult to achieve. The impact of one single action can hardly be assessed without the aforementioned context and without recognising of the mutual exchanges of intimidation tactics taking place throughout time (Steiner, 2016). All these actions and reactions, in Schelling's view, should be credible yet reversible to invite compliance and avoid humiliation (1966). Thus, coercion is more effective in a "permissive or non-mutually exclusive" setting (Javier, 2022).

At the same time, coercive diplomacy depends on communication (George, 1997), since in order to influence a state's behaviour, said state must first comprehend the coercer's motives, or in other words, what is asked of it. Taking this idea one step further, researchers have recognised another function beyond constraining target nations or demanding compliance: signalling. Economic warfare can be aimed at showing disapproval of certain policies or actions (Elliott, 2010), a gesture aimed at the direct target —be it the adversary state or its population— as well as potentially showing resolve vis-à-vis the international community. However, what constitutes signalling exactly is unclear. As an example, some researchers would include the stigmatisation of the target state within coercion efforts, separately from the senders' efforts to signal inappropriate behaviour (Jones, 2018), whereas for others it would all be a "signal". Furthermore, even if scholars reduced "signalling" to the mere aspect of vocalising a threat, separating the signalling impact of economic warfare from other dimensions would be no easy task, explaining why the topic is labelled in the academic community as under-researched.

2.2 A critical examination of other conceptualisations: cyber warfare, cyber-economic warfare, economic information warfare

Cyberwarfare and cyber coercion

For many, cyberspace, a rapidly emerging facet of modern conflict, has fundamentally transformed (if not revolutionised) the landscape of war in the digital age. Cyberspace has even been proclaimed as the fifth battlespace (Cornish, 2011).

As societies have become increasingly reliant on interconnected technology, the cyber domain has emerged as a powerful arena for state and non-state actors to engage in strategic manoeuvres and exert influence. Unlike traditional warfare, cyber warfare promises to transcend physical borders and allow adversaries to exploit vulnerabilities to launch sophisticated attacks on critical infrastructure, economies, and national security. It has opened new avenues for disruption, espionage, and sabotage, demanding novel strategies, regulations, and a great deal of research.

In the captivating world of science fiction, "cyber war" conjures mesmerising images of high-stakes AI-driven assaults and breathtaking cybernetic showdowns among ethereal virtual entities. But what exactly does this term refer to?

In recent years, the term 'cyber warfare' has gained significant prominence in discussions concerning the evolving landscape of modern conflicts. However, amidst its growing usage, a striking lack of consensus surrounds its exact definition and scope (Cornish, 2011). Various experts and scholars have put forth multiple definitions and explanations, leading to divergent perspectives on what truly constitutes cyber warfare. This lack of agreement extends to the actors involved, the specific effects required to label something as 'cyber warfare,' and the potential targets encompassed by this concept. As a result, the notion of cyber warfare remains an intricate and multifaceted subject —with contradictory definitions ranging from cyberwar's non-existence to cyberwar as an imminent threat—, hindering interdisciplinary research and policy communications (Ashraf, 2021).

A study realised by Hughes and Colarik in 2017 exemplifies the diversity of understandings and the artistic liberties with which scholars and policymakers treat "cyberwarfare". On the one hand, the research revealed that 103 out of 159 cyberwar articles sampled[3] failed at providing a proper ("explicit") definition of cyberwarfare or cyberwar.[4] On the other, the definitions provided by writers of the sampled pieces belonged to or were influenced by very different disciplines: military, law, international relations, strategy and security, ICT, etc. Hughes and Colarik also observed a correlation between the growth and decline in the research (in all likelihood also linked to assessments of its seriousness as a threat and actors' political agendas) and what can be considered as the sudden emergence of important "international cyber incidents" (2017). Although they traced most pseudo-definitions to a handful of authors, Ashraf goes one step further and classifies them into themes (or moods): scepticism, alarmism (or

[3] Their research began with 1993's Arquilla and Ronfeldt's article "Cyberwar is Coming!"

[4] They initially attributed different meanings to cyberwarfare and cyberwar, with the former understood as "the means of cyberwar" and the latter an act of war. However, the researchers eventually concluded that "the current discourse does not provide sufficient evidentiary basis to definitely distinguish between the terms" and continued their study treating the two notions as synonyms.

fearmongering), and realists (with a strong focus on norms) (2021). In the realm of cyberwarfare, alarmists perceive it as an impending and formidable threat, while sceptics challenge this notion, claiming that cyberwar should not be classified as or raised to the order of "war". According to him, some within this sceptical group also believe that cyberwar is not only exaggerated (possibly comparable to Cold War fearmongering), but it serves the interests of defence budgets and the cyber-industrial complex. Realists, however, strike a middle ground and advocate for understanding cyberwar within the context of existing laws and norms. (Ashraf, 2021).

Famously, for John Arquilla and David Ronfeldt (1993) cyberwar typically entails conflicts between organised military structures (cyberwar is a sum of military operations), whereas "netwar" would be a more inclusive term regarding nonstate actors (Gartzke, 2013). According to Ashraf, their publication "established a class of 'alarmist' definitions" that would place cyberwar as an imminent threat (2021). Other often-referenced authors are Clarke and Knake, who define cyber war as "the act of a nation-state to penetrate another nation's computer or network to cause damage or disruption". This definition also strongly constrains cyberwar to states. Rid and Gartzke also seem to prefer state-centric definitions of cyberwar, while Lindsay and Betz (2012) contend that cyberwarfare is only available to states due to their significant resources (both financial and technical) and remain doubtful that non-state actors will have the capabilities to execute cyberattacks with the necessary magnitude (Ashraf, 2021).

This is closely linked to another key discussion, which is the scale of the cyberattacks and what level of damage amounts to cyber ”war". McGraw, for instance, understands cyber warfare as the utilisation of violent and physical force by groups driven by political, economic, or ideological motives (2013). Based on this interpretation of cyberwarfare, two significant implications emerge: firstly, cyberattacks, according to McGraw, should entail a tangible kinetic effect or a discernible physical consequence; secondly, cyber warfare serves as a strategic tool aimed at accomplishing political objectives. However, when the reader looks at the examples provided by McGraw, this line of argumentation shows its weaknesses. He labels as cyberwar (virtual means, physical impact) the incapacitation through cyber means of an air-defence system which resulted in the facilitation of the destruction of the target. This unfortunate example, commonly known as "Operation Outside the Box", involved electronic warfare (which is not a synonym for cyber warfare), and the kinetic effect was ultimately brought about by fighter jets bombing a blind target. As he correctly points out, "the less straightforward part is determining whether an action with no real-world impact constitutes cyber war", but which cyberattacks do not have an effect in "reality"? But he is not alone: for other researchers seem to stand for the classic 'what happens in cyberspace stays in cyberspace'. It is considered a self-contained domain with minimal spillage into the physical realm or offline world (Valeriano and Maness, 2012).

Ashraf's criteria, in this situation, are limited in their application, as McGraw seems to be at times sceptical (arguing the threat of cyberwar is indeed overstated), while warning of its "inevitability" (bordering on alarmism) (2013). McGraw engages, in his publication, another well-known critic of "cyberwarfare", Thomas Rid. Rid believes that cyberwar would require a potentially "lethal, instrumental and political act of force", with exceptionally stringent criteria for what would fit into the cyberwar category (Rid, 2013).

He also asserts that historical occurrences, future prospects, and current circumstances collectively do not align with his concept of cyberwar. In his view, cyberwar fails to meet the traditional threshold of war, as it does not produce enough violence or casualties (Gartzke, 2013). Unlike McGraw, Rid posits that cyber war will not take place, claiming that "no cyber offence has ever caused the loss of human life. No cyber offence has ever injured a person. No cyberattack has ever damaged a building" (Rid, 2013).

Another critical, yet challenging distinction is the one between cyberwar and cybercrime. Some scholars would separate them according to the above-mentioned criteria (actors, the scope of the attack and/or damage caused…with cybercrime usually covering the lowest impact versions of these attacks), while others like McGraw consider them (together with cyberespionage) as distinctive parts belonging to a more global threat, like the heads of a Cerberus (2013). Stephen Walt gives careful consideration to the multifaceted nature of cyberwarfare, identifying four issues encompassed by this term: weakening an adversary's military capabilities, infiltrating networks to disrupt civilian infrastructure, engaging in criminal activities online, and conducting cyber espionage (2010) (Gartzke, 2013). For Datta, cyberwarfare encompasses an extensive campaign, as opposed to many cyberattacks which occur "in isolation" (2021). Datta argues that cyberwarfare rather entails a purposeful and coordinated series of cyberattacks sponsored by nation-states, characterised by an ongoing exploration and exploitation of "digital and cyber-physical vulnerabilities", to undermine a nation-state's economic and operational frameworks (2021). Brenner offers alternative reasoning: the distinction between crime (cybercrime) and war (cyberwar) becomes blurred as territory becomes irrelevant (2006). What separated the two concepts was a border, "crime" equated "internal problem" whereas war was an external threat. This is further complicated by the multiplicity of actors carrying out attacks. Alas, a final distinction is made between what he calls "routine cyberthreats" and "non-routine cyberthreats", with the former linked to cybercrime and the latter to warfare.

Nonetheless, there are additional questions beyond that of the frequency. According to Gartzke, most of the potential harm envisioned in cyberwar scenarios is likely to be temporary. He claims that, contrary to pessimistic views, the notion that cyberspace could fully replace traditional conflict is mistaken, as cyberattacks, though very costly, often have short-lived effects that can be remedied relatively easily with a "modest investment of tangible resources". For him, unlike conventional warfare, cyberwar lacks the destructive impact of physical attacks (of the likes of bombing a city and the loss of human lives) and will therefore have a shorter-term impact on its victims or targets. What he considers an impact is not entirely obvious, whether it is physical or psychological (undermining public morale), but Gartzke believes that in order to achieve its political objectives, cyberwar must complement other forms of warfare. This idea raises interesting questions regarding the role of cyber in wider conflicts: is cyber just an additional nuisance, dipping the toes and testing the enemy, or the vanguard of a larger force to come?

Lower-impact —presumably— conflict has its perks, since compromising or rendering networks inoperable could potentially grant an opponent noteworthy tactical or strategic advantages (Gartze, 2013). For Zilberman, "The beachheads of the future […] [beachhead understood as concentrating efforts in an area that can serve as a strategic foothold and a base from which to launch further operations] are being established today in cyberspace" (2018).

Another relevant aspect, perhaps intrinsic to the rationale behind cyberwar, involves the concept of influence, with an actor leveraging the capacity to inflict harm to dissuade another actor from certain policies or to achieve concessions (Gartze, 2013). This mechanism underscores how the realm of cyberwarfare operates beyond mere physical confrontation, illustrating its potential in shaping geopolitical dynamics. This is perfectly feasible by targeting the state apparatus, from its financial systems to its transportation networks (Cornish, 2011).

This is a form of cyber coercion. Steiner (2016) assesses that cyberattacks are employed in two distinctive ways: either as a tool for warfare (or strikes) or as a cost-effective instrument for coercive diplomacy. The extension of coercive action to the cyber realm is appropriate according to scholars for various reasons. For Gomez, compellence, whether initiated proactively or reactively, aligns with the preemptive deployment of cyber tools targeting an adversary, and the restraint or manner in which cyber capabilities are employed showcases a level of rationality on the side of the coercer (2018). He posits that, ultimately, "the fundamental structure of cyberspace assists, if not enables, coercive behaviour". However, as explained in the section above, coercive theory establishes a series of parameters upon which a state can coerce or compel an opponent to undertake a specific action. One of these is clearly transmitting what the desired outcome would be or what the coercer's demands are, but in practice, these signs are much harder to pinpoint.

According to Hodgson, reality tends to involve "ill-defined threats" even while stating the need for change, or the consequences might be materialised in the hands of a proxy (with coercion efforts benefitted or undermined by the double-edged sword of the attribution problem). This could significantly complicate the identification of coercion in its early phase or even over the course of a prolonged coercive effort (Hodgson et al., 2019). Moreover, the message might not be interpreted uniformly by the parties concerned. Hodgson maintains that cyberattacks' coercive potential should not be questioned through the lens of traditional understandings of coercion (2018). In theory, coercive measures, if explicitly announced with a political objective, should prevent the enemy from preparing for the attack. Nonetheless, the specifications provided would be, more often than not, far from enough to fully pre-empt the actions. Furthermore, in Hodgson's words, "the growing vulnerability to cyberattacks [given the increasing digitalisation of societies] means that the prospective attack surface is so large that adequate preparation is unlikely". He also challenges another common assumption: the announcement of the means that will be employed in the process of threatening the opponent: a state does not need to give detail to be credible, only to be known to have the capacity to inflict harm (2018). This being said, there are disagreements on whether cyber operations can be used in the usual form of "signalling". Take for example the affirmations of Valeriano. He states that the efficacy of cyber operations is a priori maximised when conducted with a shroud of secrecy and deception, since it enables "escalation management" (Valeriano, 2018). At the same time, he also argues that "cyber operations [most commonly] act as ambiguous signals associated with tacit bargaining (…) or help a rival state alter the balance of information (through espionage as a means of gaining an intelligence advantage)". For him, only a small portion of cyber operations would align with conventional coercive acts of “degradation” to compel adversaries (Valeriano, 2018).

Considering these disagreements, it is not surprising that Hodgson would define cyber coercion in an inclusive and open manner. Cyber coercion is described as “the threat (implied or explicit) or limited use of cyber operations to motivate a change in behaviour by another actor that may involve cyber operations on their own or in conjunction with other coercive actors” (2018). But of course, there are those who would still claim that anything and everything is “asking too much of cyber” (Lonergan and Poznansky, 2023). The disadvantage faced by such dissenting voices is that, by focusing on its effectiveness, they will fail to adequately estimate the frequency at which enemies attempt to perform (for lack of a better word) cyber coercion and the damage inflicted in the process (Lonergan and Poznansky, 2023). Despite coercion’s allure, effectively achieving it remains a daunting goal.

In Hodgson’s opinion, to determine whether a cyber operation is, in fact, part of a wider coercive strategy, one should track the enemy’s capabilities (those demonstrated in the past and where it is heading in the future given its resources), reflect on the broader context of the cyber operations (developing conflicts), and identify the coercer’s demands over time (Hodgson, 2018). These operations do not manifest independently, in isolation, but they are part of a broader framework, integrating an amalgamation of diplomatic, economic, cyber, military, and other tools. Valeriano would add to this list of warning signs two other relevant points, including the time window for malicious intent (taking into account the coordination between evoking behavioural change and the beginning of the cyber operation) as well as the target selection.

Cyber-economic warfare

Cyberspace has profoundly reshaped the contours of economic warfare, ushering in a paradigm shift marked by novel tools, means, and an ever-increasing, accessible and exploitable platform. In this expanded framework of economic warfare, the cybersphere assumes a pivotal role, enabling the targeting of all economic assets and critical infrastructure of the opposing party. As all industries continue their digital transformation, cyberattacks not only emerge as a distinct weapon within the arsenal of economic warfare for states but also serve as a catalyst, amplifying the potential harm that a nation can inflict on an adversary's economy. Globally, they can impact the economy on a micro and macro level (Smolanoff and Greene, 2023). At the micro level, these attacks infiltrate individual businesses, compromising sensitive data, disrupting operations, and imposing financial burdens through theft or ransom demands. Such intrusions can lead to a long list of consequences: reputational damage, legal expenses, potential customer attrition, and can seriously undermine a company's bottom line. On a larger scale, cyberattacks reverberate throughout entire economies. The alarming projection that costs linked to cybercrime could soar to a staggering $10.25 trillion annually worldwide by 2025 (Smolanoff and Greene, 2023) illustrates the mammoth financial implications of these attacks. Beyond monetary losses, cyber incidents can erode public trust, destabilise industries, societies and countries and influence international geopolitical dynamics. The interconnected nature of modern economies only amplifies the ripple effects of such attacks, with state and non-state entities exploring novel avenues and new vulnerabilities (Ravich, 2015).

As technological advancements amplify the potential impact of cyber intrusions on economic stability, there is an increasing imperative to delve deeper into the intricate interplay between these domains, i.e. economic warfare and cyber warfare. Perhaps the most solid conceptualisation of this marriage is the one provided by researchers at the Foundation for Defense of Democracies. They use the term "cyber-enabled economic warfare" to refer to those "attacks against a nation wielding cyber technology with the specific intent to weaken its economy and thereby undermine its political and military power" (Ravich and Fixler, 2017). This approach allows for a more comprehensive understanding of the adversarial strategy behind cyber incidents which at first sight might appear unrelated. At the same time, it presents economic warfare at the centre of this strategy (beyond tactical and operational choices in cyberspace). Ravich and Fixler offer a pretty straightforward checklist through which scholars can to a certain extent separate the wheat from the chaff. For them, an attack or attacks constitute cyber-enabled economic warfare insofar as it: a) is cyber-enabled (as opposed to electronic warfare); b) causes or is aimed at causing economic harm; c) the economic impact is important enough to have the potential to "degrade national security capabilities"; and d) is strategically oriented towards eroding a state's national security (Ravich and Fixler, 2017).

At the centre of the aforementioned research are these key questions: what if the changing and rising cyberattacks that are often dismissed as cybercrime actually integrate a wider strategy to undermine a country significantly? What if the rationale behind it exceeds financial gain and is aimed towards the progressive erosion of a country's economy? What if ongoing attempts at provoking economic harm are the prelude to debilitating a country's security capabilities? (Ravich, 2015). Shulsky expands on this idea, introducing an array of potential avenues leading to cyber-enabled economic warfare, from cyberespionage to cyber-sabotage or disruption of a country's economic and financial infrastructure, for example, by targeting critical infrastructure (2015). Shulsky would include among this threat the dissemination of disinformation, particularly aimed at eroding confidence in the country's main economic institutions, and questioning their credibility and stability. He believes disinformation could be used to cause a particular reaction from financial markets and instil panic in the population. However, he pays particular attention to cybersabotage, identifying those situations in which the situation might not constitute economic warfare, but a wider issue:

> "the effects could be so widespread and damaging as to constitute [...] an act of war, against which [the victim] might feel compelled to retaliate. [...] If the cybersabotage were able to do extensive physical damage to the infrastructure, then the victim might be weakened economically for a considerable period of time. [...] It is likely that action of this sort would be undertaken as a prelude to all-out-kinetic-warfare."

These cyberattacks are scarce. Shulsky rightly points out that in most instances, the damage, even if important, would probably be reparable after a while, allowing the victim to recover "economic strength". One could therefore deduce that most actions of this type, cybercrime, would hardly by themselves reach the threshold of economic warfare and lead to major economic instability. Yet the collective outcomes of these endeavours could effectively diminish the target's economic stability and erode trust (such as the citizens' trust in both the government and the entities targeted) over time. Although perhaps of secondary significance to the previous point, attacks like ransomware could also provide an alternative stream of revenue for the attacker state to continue financing its international 'commitments' and further criminal activities. Still, Shulsky admits that for a long-term strategy of this kind to ultimately lead to a devastating (economically too) "cyber Pearl Harbor", the attacker would necessitate a level of sophistication and coordination that current nation-states (referring mainly to Russia and China) might not yet possess (2015).

Cyber-enabled economic warfare is still developing in scope, with researchers finding new connections between cyber developments and malicious economic statecraft. Hsieh denounces, for instance, the extensive cyber-driven appropriation of intellectual property, which bolsters the adversary's domestic economy by leveraging the research and development investments of the targeted economy (2015). And warning bells have been ringing for a decade: in 2012 the director of the US National Security Agency described this phenomenon as the "greatest transfer of wealth in history" (Rogin, 2012). From this perspective, the symbiotic convergence of motives of profit-seeking groups with the strategic objectives of states to acquire technological expertise (through illegal means) is far from coincidental and has its historical precedent in privateering.

Economic information warfare

With information at the centre of states' concerns, there is an alternative lens through which the convergence of economics and cyber can be studied: "economic information warfare". It stems from the concept of "information warfare", which would encompass a series of tactics and techniques weaponised in the information realm to secure a competitive edge over an adversary during a period of high tension or conflict (Brazzoli, 2007; Stupples, 2015). Scholars describe economic information warfare as a series of actions aimed at, among multiple things, controlling and disrupting economic operations through the manipulation of information and information systems (Chatterji, 2008). This phenomenon would block or impede the smooth flow of economic information, akin to a blockade (Chatterji, 2008). Although this theory might initially lead the reader to believe this is a more sophisticated form of describing disinformation operations online, there is an additional angle. Hutchinson and Warren have identified a trend among activities like data destruction, data corruption and manipulation, data theft, and disruptions in access to data, eventually influencing public perceptions of such data and altering its context (2021). These procedures are at the core of most cyberattacks targeting organisations, with cybersecurity experts focusing on safeguarding what is commonly known as the CIA triad: the confidentiality, integrity and availability of data.

However, the term information warfare triggers its own set of difficulties, battle spaces, subsections and types, of which, according to some scholars, economics or cyberwarfare are only a fraction (Libicki, 1995). The same can be said about economic information warfare, which can be applied as much in the physical (in addition to playing with perceptions) (Deakin, 2003), as in the digital realm.

2.3 Cyberattacks as geoeconomic instruments and tools of economic warfare

Before delving into reinterpretations of cyberattacks in the context of economic warfare, it is important to recognise the lack of a single unchallenged definition of "cyberattack" and a clear distinction of what actions exactly are encompassed under this term. Such discussion, while it remains outside the scope of the dissertation, is understood by this author as the beginning of many theoretical obstacles and the root of the lack of conceptual clarity in the field of cybersecurity and cyberwarfare. However, in order to establish a framework for the primary theories utilised in this dissertation, the subsequent definitions are provided. The CSRC-NIST Computer Security Resource Center describes cyberattacks succinctly as "any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself". According to Chatham House, most cyberattacks can be reduced to a "deliberate entry into a computer system with malicious intent" —threatening individuals, businesses, and governments—, yet the term also describes "politically motivated attacks" (2022).

Blackwill and Harris define the concept of geoeconomic cyberattacks as "those making use of economic or financial market mechanisms and seeking to impose economic costs as part of a larger geopolitical agenda" (2016). They introduce cyberattacks as a geoeconomic tool, insofar as these have the explicit endorsement (sponsorship) or planning of a state to undermine or jeopardise the critical economic/financial infrastructure or major economic/commercial entities of another state, and ultimately lead to tangible or potential geopolitical advantages (Blackwill and Harris, 2016). This is consistent with the very definition of cyberattack provided by Hathaway —"Any action taken to undermine the functions of a computer network for a political or national security purpose"— (2012).

Against this backdrop, critics have voiced that while a cyberattack targeting critical infrastructure can undoubtedly inflict economic harm and represent a national security threat, it does not imply the utilisation of economic methods to achieve geopolitical objectives. Troxell, for instance, argues that "the examination of this aspect of statecraft should have its own platform and not necessarily be considered a geoeconomic event" (2018). From this perspective, cyberattacks with a geoeconomic motivation would still be subjected to a wider military strategy (in the traditional sense). Likewise, Troxell believes all cases to be submitted to the same rationale as an exception mentioned by Blackwill and Harris, whereby bombing a factory would not be included within geoeconomics despite constituting an economic target (2018). Blackwill and Harris are aware of the challenge of navigating liminal cases: they believe that what distinguishes the factory bombing from geoeconomics is not its arguable economic character, but the fact that military targets belong to a distinct sphere of norms and practices of war. While geoeconomic statecraft can appear during wartime, geoeconomic techniques "stand as an enterprise substantially separate from questions of military targets and warfighting strategy" in its classical form (2016).[5]

Blackwill and Harris (2016) illustrate this complexity by presenting various scenarios and examples. One such instance of geoeconomic cyberattacks involves the 2007 Russian

[5] This distinction is also present in the research of Ravich and Fixler, who differentiate cyber-enabled economic warfare from cyberwarfare precisely due to the fact that the latter is focused on "directly degrading military capabilities", as opposed to being "intended to cause economic harm as a way to indirectly degrade national security categories" (2017). The emphasis here is on how straightforward the aim is, or whether the goal is achieved through a secondary platform (the state's economy).

government's attempts to assert dominance and exert geopolitical influence over a neighbouring country, Estonia, with which it was not openly in conflict —as opposed to Russia’s July 2008 cyberattacks against Georgia’s Internet infrastructure in (given the hostilities over South Ossetia). Another telling example would be an attack on a major internet service provider: if the aim was to access specific emails, it might not be geoeconomic; if the intent is to undermine its functionality or cause widespread economic disruption through internet outages, it can be classified as such (Blackwill and Harris, 2016).

This discussion is relevant since, even in forums where there seems to be greater recognition of economic cyberattacks (mainly in the U.S.), there is no consensus on which cyberattacks constitute economic warfare (Ravich, 2015) —mirroring scholarly difficulties in defining what is a cyberattack—. Blackwill and Harris note similarly to other types of economic statecraft, geoeconomic cyberattacks vary in form and objective: some focus on data theft or industrial espionage, and others are retaliatory in nature (2016). For Ravich, examples of “malicious cyber-enabled actions against economic targets” are grouped into four categories: cybercrime (like fraud), cyberespionage (like intellectual property theft), cybersabotage, cyberterrorism (2015) and cyber-enabled information war (2017). Ravich and Fixler, unfortunately, failed to classify several important cyberattacks as cyber-enabled economic warfare claiming that “more information [was] needed”. These included the 2008 sabotage of the Baku-Tbilisi-Ceyhan pipeline prior to the war between Russia and Georgia (which counted with Russia’s opposition), the sabotage of Iran’s energy sector in 2012, “Russian back doors” through technology firms and the state’s connection to cybercrime, as well as the sabotage of Ukraine’s electric grid in 2015. Interestingly, Russia seems to be at the centre of all doubts, with scholars often demanding further indisputable proof of Russia’s intentions and linkages between incidents and Russia’s cybercriminal networks. Given difficulties in attribution, the nature of cyberattacks, and more generally how countries – in particular Russia – utilise plausible deniability extensively in their conduction of international affairs, these scholars will likely never be fully certain. However, it must be highlighted that in Russia´s case there exist a substantial amount of evidentiary “clues”, underpinning the well-grounded speculations regarding Russia´s continuous interference. Despite these indices individually failing to reach the threshold of being fully attributable or interlinked, this thesis finds that they collectively create an image which points squarely at Moscow. While analyses of international behaviour are often drawn from assumptions, this should not be misinterpreted to mean that we are clueless.

With cyber operations increasingly being viewed as a supplementary tool within foreign policy, it would be important to agree on some common terminology to identify behaviours and respond accordingly. Regrettably, it is hard to find a global taxonomy regarding cyber operations (leaving the economy aside). Gomez establishes a simple yet useful classification of said operations on the basis of intent, distinguishing between disruptive cyberattacks, espionage, and degradative operations (2018). Disruptive operations have the objective of disturbing the normal functioning of the target, employing DDoS attacks or defacing websites. Since the tools needed to carry out these attacks are usually accessible, they are easily detected or managed and their impact is limited and of short duration. According to Sueur and Juijkx, disruption has two ends: 1. Financial reward, as is the case with ransomware attacks (with varying levels of sophistication, they can be average or standard attacks, appear very opportunistic or target carefully selected victims employing advanced techniques), and 2. Temporary disablement, impairment and destruction (manipulation of information, rendering it inaccessible etc.) with the expectation of gaining a tactical advantage (2022) —probably finding its roots in (geo)politics. For Gomez, the latter would rather be representative of degradative cyber operations, which attempt to disable or seriously damage the cyberinfrastructure of the adversary. The intent of degradative operations is to hinder a state's strategic interest by triggering cascading effects into multiple connected sectors. The consequences span beyond any technical malfunctioning, and thus, for Gomez, are "ideal for coercion" (2018).

These two situations in reality often overlap, with APTs often perceived to have significant foresight along longer timeframes, through maintaining extended access to critical infrastructure (or rather, the organisations maintaining them). This is further believed to serve as a form of insurance policy to allow the offensive nation behind the APT to apply pressure on the targeted nation (Sueur and Juijkx, 2022).

This dissertation builds on all previous concepts, but particularly on the theory of cyber-enabled economic warfare, identifying the potential of the instrumentalisation of economic warfare and cyberwarfare simultaneously to coerce an adversary into modifying its geopolitical stance.

In sum, this dissertation develops the idea that some cyberattacks are deeply strategic and are integrated into a greater plan (statecraft) —as opposed to reflecting isolated events—, whose goal is to coerce the enemy into refraining from or changing certain actions. The goal is political at its core, sending a message about the coercer's expectations, demands, and limits. The pressure is exerted through digital technologies in the cyber realm, where most of the activity of the economic sector occurs. According to Even, cyber-based broad economic warfare also "impair(s) governance and damage(s) the economy and state's income", given the role of digital platforms in establishing and maintaining connections between citizens and businesses, and businesses and governments (2018). The chosen targets are varied in nature, from private companies to public agencies in critical sectors of the economy, impacting the financial situation and public confidence in the company, the nation's economy, and connected institutions. The attacks are designed to disrupt, damage, influence and weaken a state's economy, and the perpetrators are numerous, with state and non-state actors.

3. ANALYSIS

3.1 Context

Europe-Russia relations: the role of energy

Russian and European energy needs are highly interdependent. Europe's diversified economy requires substantial imports from Russia, while the Russian economy, dependent on natural resource extraction, needs export revenues from Europe (Delorme et al, 2022). However, contrary to the expectations of liberal theories, this interdependence has exacerbated mutual security tensions (Krickovic, 2015). Although

Russia and the EU are often thought to be mutually dependent on one another as buyer/supplier of energy, this is a grave oversimplification, and fails to acknowledge Russia's upper hand in the relationship (without great efforts from the EU states) (Kardás, 2023).

Russia ́s coercive practices have allowed it to maintain a high level of unpredictability, which it can leverage for geopolitical gain (Busygina, 2017). As an example, it has balanced both an economic openness to the West (largely due to the need for FDI), with a political distancing from it (Busygina and Filippov, 2013). Within this approach to international affairs, energy is considered a weapon, used to pressure sovereign states (LaBelle, 2023). This weaponisation of energy can thus be considered an example of economic warfare (Blank and Kim, 2016).

Natural gas, oil, and nuclear energy became the ammunition to feed this weapon. As Moscow openly recognises those assets as major instruments of Russian foreign policy, being seen as vital to the enhancement of Russia's global power, influence, and standing, it has leveraged them extensively against its neighbours —Eastern and Central Europe, and the CIS. (Blank and Kim, 2016)

This weaponisation of energy traces back decades. In 1990, Moscow – then helming the Soviet Union – halted its oil supplies to the Baltic states to undermine their burgeoning independence movements. In the years since, Russian energy companies, most likely with the Kremlin's acceptance or guidance, have repeatedly sought to leverage their resources to advance Moscow's strategic priorities. Although concessions were occasionally given, these coercive practices actually drove the targeted countries further from Moscow's orbit. Lithuania and Ukraine stand as two examples of countries which, reacting to Russia's disruptions, sought to strengthen and rebuild their supply chains, increasing their resilience and decreasing their reliance on Russia (Collins, 2017)

Russia heavily relies on its abundant non-renewable energy resources, including oil, gas, and coal, which make up over 60% of its exports (Sueur and Luijkx, 2022). These exports have been growing rapidly in the decade leading up to the Ukraine war - Russia's share of total EU gas demand increased from 26% in 2010 to over 40% through 2018-2021 (International Energy Agency, 2023). This grants Russia significant geopolitical leverage over Europe. However, Russia is reliant on foreign technologies to modernise its energy industries, which has been hindered recently due to international sanctions (Sueur and Luijkx, 2022).

Russia's utilisation of energy as a coercive instrument has functioned as a geopolitical tool across numerous former Soviet Union states since the early 1990s. Since Vladimir Putin took power, energy has consistently served as a strategic method to achieve Russia's foreign policy objectives. In the first half of the decade of the 2000s, Russia suspended energy exports on approximately 40 instances, with the CIS and central and Eastern Europe being primary targets (Grigas, 2012).

Suspending energy exports is not the only method which the Russian government utilises. In 2006, Russo-Ukrainian negotiations led to major Ukrainian geopolitical concessions —including postponing any referendum on NATO membership and the continued hosting of the Russian Black Sea Fleet in Crimea. In exchange, Russia guaranteed lowered gas prices (Kardás, 2023). And in Central Europe, Russia has sought to use its energy exports to sow discord and undermine Western Europe's influence. It seeks to influence and entice alignment with the former Soviet bloc, while cooperating and trading with the governments of the West. In these efforts, Gazprom has served as a notable actor (LaBelle, 2023).

Europe, Russia and the War in Ukraine: involvement and the worsening of relations

The European Union, and certain other Western countries have been steadfast in expressing support for Ukraine and threatening severe economic and political consequences, in response to Russia's aggression (European Parliament News, 2022). Leading MEPs strongly criticised Putin's recognition of Donetsk and Luhansk, as well as the fully-fledged attack on Ukraine two days later (European Parliament News, 2023).

Between the first package of sanctions on the 23rd of February 2022, to the eleventh package in June 2023, the EU has imposed multiple rounds of sanctions and taken strong action against Russia in response to its aggression, including measures like banning transactions with Russian banks, a proposal to ban all Russian oil imports, declaring Russia a state sponsor of terrorism, and implementing a strict cap on oil prices (European Parliament News, 2023). The European Peace Facility (EPF), a fund initially valued at €500 million (European Council 2022a) and later increased to €3.1 billion (European Council 2022f), was established in February 2022 to provide military aid to Ukraine, particularly for equipment and maintenance, signifying a significant investment by the European Union (Trebesch et al., 2023).

Furthermore, some countries, such as Germany and Sweden, have reversed their prior commitments to not export lethal military aid, to better supply Ukraine. The European Union, for the first time ever, supplied lethal arms through its institutions, with all EU member states contributing military aid except for Hungary, Cyprus, and Malta. In January 2023, the combined pledged support of all EU member states and institutions had reached €54 billion —with around 40% of this being bilateral commitments from individual member states, and pledges from the EU Commission and Council constituting the other 60%. The UK ranks as the second-largest military donor globally in terms of pure monetary value, with in third place. Germany, the Netherlands, Italy, France, Denmark, Sweden, and the Czech Republic also contribute significantly, and collectively, EU countries have committed almost as much heavy weapon aid as the United States, excluding ammunition and other such supplies. Whereas the largest bilateral contributors in pure monetary value are the UK and Germany, (alongside the EU and the US), Eastern European countries have donated more as a percentage of their GDP. These include Estonia, Latvia, Lithuania, Poland, the Czech Republic, and Bulgaria, which furthermore have each committed more to Ukraine through direct bilateral aid than through the EU. Ultimately, in terms of crucial weapon systems, Europe has contributed significantly more than the available aid data indicates. However, it's important to note that European governments have allocated significantly greater resources to protect their citizens from the impacts of the war and energy crisis than what they have allocated to support Ukraine. (Trebesch et al., 2023)

The 2022 invasion of Ukraine by Russia disrupted the post-Cold War European security order and fundamentally altered the EU-Russia relationship, formerly based on economic and energy interdependence. However, Russia is now regarded as the foremost threat to European peace and stability, resulting in a strained relationship centred on security. The past half-century of mutually beneficial energy relations has ended, with EU member states actively severing economic ties with Russia. However, there were always underlying tensions, stemming from Russia's power struggle and competition with the EU over Eastern Europe. Russia's attempted subjugation of Ukraine is only further diminishing its power and bolstering European unity (Meister, 2022).

EU-Russian relations have been deteriorating since Russia's annexation of Crimea in 2014 and interference in Eastern Ukraine. This led to EU sanctions, Russian countersanctions, and a decline in trade. Despite this response, EU member states were divided on how to engage with Russia, with some hoping for "constructive cooperation" on specific regional issues "when conditions allow". This ambiguity reflected the desire of certain states, including France, Germany, Italy, Austria, and Hungary, to improve relations with Russia, making it challenging to distinguish between compromise and appeasement. European unity was further undermined by Russian disinformation campaigns, cyber-attacks, and media manipulation (Meister, 2022).

The entangled interdependence of energy, economies, and trade failed to prevent the war's outbreak. Rather, Putin believed that the EU was too dependent to impose substantial sanctions —a belief which has since been fundamentally shattered. While the EU is (almost unilaterally) united in applying sanctions and aiding Ukraine, there is no shared strategy for future engagement with Russia. Its recent move to grant (potential) candidate status to Moldova and Ukraine underscores heightened geopolitical competition with Russia. The EU's near-term policy toward Russia will prioritise self-defence against disinformation and hybrid threats, military deterrence, and decreasing economic and energy reliance (Meister, 2022).

Since February 24, 2022, Germany has significantly shifted its stance towards Russia, revising its assumptions about Russian intentions and supplying weapons to Ukraine. Berlin has enacted tough sanctions, halted most trade with Russia (in particular, fossil fuels), and redefined its energy policy, while committing more to defence. Trust in Russia is so eroded that only concrete, short-term agreements are viable, with contingency plans for potential Russian non-compliance (Stewart, 2023). This pattern is resonating across Europe, with countries including Poland, Slovakia, Bulgaria, Belgium, the Netherlands, Ireland, and Czechia, all expelling Russian diplomats for alleged espionage (Intellinews, 2023).

Europe's Energy Sector in 2022

In the decade leading up to the February 2022 invasion, Germany grew increasingly energy dependent, with Russia seeing this as a prioritisation of economic interests above all else. However, Germany's ending of the Nord Stream 2 project in February 2022, its significant military aid contributions to Ukraine, and its support of major sanctions packages, dispelled this notion. Subsequently, Russian gas deliveries through Nord Stream 1 were reduced and eventually halted entirely in September. Sabotages on both

Nord Stream pipelines occurred, coinciding with the opening of the Baltic Pipe for gas supply from Norway, rather than Russia (Fix, 2023).

Since the February invasion, the top five importers of Russian fossil fuel have been Germany, Netherlands, Italy, Poland, and France. Italy heavily relies on gas, comprising 42% of its energy consumption. Of this gas, 45% is imported from Russia. The Netherlands, with a lower dependence of around 15% on Russian gas, plans to cease Russian energy imports by the year's end (Czyzak, 2022). Europe has been well aware, since the invasion began, that reducing its reliance on Russian energy was vital for undermining Moscow's profits and leverage. As such, coal and other solid fossil fuel imports were banned in April, alongside a June ban on crude oil and refined petroleum. As a result, Russia has cut 80% of its gas exports to the EU (Yanatma, 2023). This is also strategic in nature - Russia's decision to halt gas supplies to Poland and Bulgaria, citing payment demands in roubles, appears to be a strategic move aimed at influencing European sanctions decisions on Russia and undermining European unity, sowing disagreement over the rate of decoupling. This exemplifies economic coercion as a Russian tool (Hackenbroich and Medunic, 2022). However, much as in the examples of Lithuania and Ukraine above, Russia's energy weaponisation has led to an active diversification away from Russian oil and gas. The Baltic states, Bulgaria, the Netherlands, and Poland are halting their gas contracts with Gazprom. Italy is looking to Algeria, while Germany is pursuing alternative energy sources through LNG and hydrogen deals with Qatar, alongside renewable energy initiatives (Shagina, 2022). By the end of 2022, Russia's position as an energy exporter had dwindled, from being the leading supplier of nine energy products to only two (Balteanu and Viani, 2023).

Regarding Europe's dependence, Russia supplied approximately a third of the EU's oil and over 40% of its gas, with OECD Europe taking in 60% of Russia's oil exports (Hackenbroich and Medunic, 2022). More specifically, measured in 2020, Bosnia and Herzegovina, Serbia, Finland, Latvia, Estonia, Bulgaria, Slovakia, Croatia, and the Czech Republic each sourced over two-thirds of their gas from Russia. Austria, Greece, Germany, Italy, Lithuania, Poland, and Hungary also relied on Russia for over 40% of their gas each. The UK, by contrast, only imported 5% of its gas needs, and limited oil, from Russia (Delorme et al., 2022).

Despite its dependence, the EU pledged to swiftly phase out Russian fossil fuel imports in the March 2022 Versailles Declaration. Although Russia more than halved its gas exports throughout the year, the European gas market remained robust. Countries achieved over 95% storage capacity by increasing non-Russian supplies and reducing consumption, causing Russia's share of European gas demand to drop from 23% in 2022 to under 10% in January 2023. Additionally, the EU imposed a coal ban from Russia and implemented a similar restriction on Russian seaborne crude oil exports, as mentioned above (International Energy Agency, 2023). The EU's new REPowerEU strategy seeks to drastically cut gas imports from Russia by late 2022 and achieve complete independence from Russian fossil fuels well before 2030 (Wolff, 2022). Its success is exemplified by Germany's complete independence from Russian imported gas (where it had previously been Europe's largest importer) (Kardás, 2023).

The invasion's effect on international markets has been tremendous. In March and April 2022, IEA member countries took the unprecedented decision to release emergency oil reserves to alleviate market pressures and assure a stable supply amidst Russia's invasion, releasing a total of 182.7 million barrels on two occasions (International Energy Agency, 2023). The disruptions in energy costs have been felt in developing economies across the world, despite hitting Europe the hardest in terms of cost (Birol, 2023). In the first quarter of 2022, European electricity prices hit record highs —the European Power Benchmark averaged €201/MWh, marking a 281% increase from Q1 2021. Spain, Portugal, Greece, and France saw the most significant year-on-year price spikes, with Italy reporting the highest quarterly average of €249/MWh, a 318% increase from the same period in 2021 (European Commission, 2022). Gas prices, meanwhile, have eased from their summer highs but still hover at over six times the pre-war average (Gros and Shamsfakhr, 2022).

These unprecedentedly high spot gas and coal prices, along with oil exceeding $100 per barrel in mid-2022, have caused a surge in electricity costs worldwide, adding enormous inflationary pressures. Governments, primarily those of advanced economies, have committed over $500 billion to protect consumers from energy shortfalls (International Energy Agency, 2022). In the EU, member states have adopted resolutions to share their strategic energy storages in solidarity, and have €674 billion, to shield businesses and consumers from increasing energy expenses, with Germany alone receiving €264 billion of these (Sgaravatti et al., 2023). The breakdown of Russia-Europe energy flows has led to a reorientation of international energy trade. The severity and complexity of this energy crisis is impacting household and industry economies globally —hindering affordable access to electricity and posing risks of a global recession (International Energy Agency, 2022).

3.2 Understanding Russia

Cyber economic warfare: identifying a strategy and precedents

Cyber economic warfare is increasingly evident in Russian cyber strategies. However, more in-depth analysis and intelligence gathering might be required to fully grasp its integration within Russia’s military doctrine (Zilberman, 2018). Russian cyber operations have traditionally been mostly focused on political or military targets, but Europe is already experiencing the effects of this strategy aimed at undermining nations' economies and, consequently, their military capabilities (Zilberman, 2018). Regrettably, only a few denounce how little attention the phenomenon has received and emphasise this shift in target selection, (Tully and Weber, 2022) with cyberattacks increasingly aimed at critical economic assets. In the last ten years, Russia has increasingly intensified its efforts, designing coordinated hybrid campaigns (including cyber operations), as can be observed in the case of European energy security. One of these instances can be found in 2020, when Berserk Bear, a suspected Russian APT group with connections to the FSB, compromised several German energy companies (Lyngaas, 2020). This was not the first time, as similar attacks against German utilities had been linked to them and American energy companies two years prior. Beyond Germany and the US, Russian-backed cyberattacks have targeted energy infrastructure in other countries, including Poland and the UK. Interestingly, these campaigns have often coincided with other incidents or threats, whether it is disinformation operations or interruptions of natural gas supplies (Dupuy et al., 2021).

When it comes to economic warfare, Russia has a longer record. According to Iskandarov and Gawliczek, starting in the late 1990s, Russia employed a range of mixed warfare strategies to weaken Georgia's sovereignty and set the stage for Moscow's influence over two separatist regions (which would eventually lead Russia and Georgia to war in 2008) (2022). One of these strategies was economic coercion, the other was a constant barrage of cyberattacks from July until a ceasefire was agreed upon in August. Ukraine is another prominent example. Ukraine's economy was flagged (prior to the invasion in 2022) by scholars as particularly vulnerable to economic warfare, given its reliance on Russian gas and oil supplies (Slukhai, 2018). Russia commonly used trade relations for political leverage, influencing Ukraine's decisions on matters like membership in the Commonwealth of Independent States, the placement of the Black Sea Fleet, NATO accession, and control over Ukrainian gas pipelines. As part of this strategy, Russia offered economic incentives to Ukraine when it aligned with pro-Russian policies, but retaliated if Ukraine pursued a different political course. One such example would be the Kharkiv agreement of 2010, which extended the presence of the Russian Black Sea Fleet in Ukrainian Sevastopol for 25 years in exchange for a $100 gas price discount (Slukhai, 2018). Russia additionally employed economic warfare, as well as cyberattacks, to induce panic and social unrest in Ukraine's society, aiming to install leaders and political parties aligned with Russian interests. From Slukhai's perspective, coercive measures used to be relatively sporadic and targeted specific sectors/markets, but from 2014, these actions morphed into what he describes as "total economic warfare".

Dupuy provides additional proof of Russia's leverage of its economic clout, particularly in the realm of energy, for political support or influence (2021): in Germany, Russia employed commercial and political connections, along with "suspected malign influence", to promote the controversial Nord Stream II pipeline project valued at approximately €12 billion. More recently, Russia-state-owned Rosatom became involved in the expansion of the Paks Nuclear Power Plant in Hungary, and is now, together with French companies, working on the construction of several new nuclear reactors (Chastand et al., 2023). Russia's strategy has proved successful, since Europe has been reluctant to target in their sanctions Russia's nuclear exports due to their role in nuclear power generation (Mendoza and Litvinova, 2023).

Regarding Russia's cyber policies and cyberwarfare attempts there is even more written. Russian cyber operations are deeply entwined with their broader approach to information warfare, as indicated by (Wilde, 2022). In Russia's strategic and military terminology, the term "cyber" is infrequently employed. Instead, they prefer the concept of "information confrontation" or "information war," encompassing a wide spectrum of activities, including both technical and psychological elements, which can be deployed against adversarial systems and decision-making processes. (Wilde, 2022). Offensive cyber activities in this context constitute just one facet of a more extensive strategy within the information environment (Hakala and Melnychuk, 2021). The aim is not solely to achieve a technological impact but also to exert a psychological one. Whatever the name, cyber or information operations align with Russia's strategic doctrine as articulated by General Valery Gerasimov in 2013 (Zilberman, 2018). Following this doctrine, a state must leverage all facets of its power, encompassing cyber and information operations, to accomplish political objectives and erode the capabilities of Russia's adversaries (Zilberman, 2018). Considering that the "national strength" of said adversaries is found in their joint economies (Zilberman, 2018) (as is the case with the European Union member states), it is not surprising that this becomes an important target of the Kremlin's cyber operations.

According to Thornton and Miron, the Russian military employs offensive cyber operations as a form of "manipulation of people's minds" to, in the long term, weaken, destabilise, and undermine their adversaries from within (2022). They assess that most cyberattacks (the "cyber-technical" aspect of "information operations") are currently kept at a low level so that they remain below a certain threshold. All these operations are, at their core, "active defence" measures, employing non-kinetic means to neutralise the enemy. Otherwise, these would, "however deniable, invite retaliation (including in the kinetic realm)". Nonetheless, Thornton and Miron identify a longer strategy. For them, such attacks are intrusions aimed at preparation for future (more damaging) activities (2022). But looking at events in Russia's neighbouring countries in the last decade show this cannot be said of all cyberattacks. While cyber operations might have been initially designed to remain below the threshold of physical damage while still undermining social cohesion, shaping behaviour and influencing foreign populations (Hodgson, 2018), between 2015 and 2016 the world witnessed a much different reality. Soon after Russia's annexation of Crimea, Russia executed a series of highly sophisticated attacks on Ukrainian energy infrastructure. These malicious attacks, which situated Ukraine as a testing ground for Russia's cyber capabilities, resulted in blackouts and the loss of heating for numerous Ukrainian cities (Hakala and Melnychuk, 2021). Moreover, in 2017, entities associated with the Kremlin deployed the NotPetya attack, which rapidly propagated across a substantial portion of the globe. This cyber offensive impacted a minimum of 300,000 computers and remains renowned as one of the most formidable cyberattacks in history (Pascual, 2023). These were all traced back and attributed to Russia's intelligence services.

Nowadays, a significant percentage of Russia's offensive cyber capabilities can be attributed to the "world of cyber criminals", rather than exclusively to its military and security services directly (Wilde, 2022). This "symbiotic relationship", which other researchers have summarised as "Russian cybercrime in Foreign Policy" (Recorded Future, 2021), is utilised to harness their combined coercive and disruptive potential (Wilde, 2022). A clear illustration of this connection is when the ransomware groups DarkSide, Revil, and Avaddon temporarily ceased their extortionist operations around the initial encounter of US President Joe Biden and its Russian counterpart in Geneva in June 2021, after which the attacks resumed (Recorded Future, 2021).

State relations with hacking groups and allegiances

It is a well-known fact that in the last decade states have adopted a growing trend of outsourcing various aspects of their activities to non-state entities, commonly referred to as "proxies." This is also the case with cyber expertise and cyber operations. As observed by Canfil, these proxies would typically operate under central coordination, with their actions directed or overseen by the sponsoring state (2022). However, scholarly analysis has identified a spectrum of relationships that states may have with these non-state actors, ranging from complete disavowal or abeyance at one end to centralised command and control at the other. On one hand of the spectrum would be Maurer (2018), who identifies three strategies (delegating, funding –orchestrating–, and tacitly permitting –sanctioning–), and on the other scholars like Healey (2011), who identifies 10 different types of arrangements. Maurer believes that this proxy would be conducting or contributing to offensive operations enabled by a state actor (the beneficiary) knowingly, either passively or actively (2018).

These divergences are explained by the intricate array of entities integrating the Russian cyber threat actor landscape: from private organisations (criminal groups and activists) to the more traditional security apparatus (military, intelligence etc.) (Soldatov and Borogan, 2022). The dynamic interplay among these actors has undergone significant shifts in recent years, with Russia fostering an environment that has not only fueled cybercrime abroad but also led to a “cybercrime epidemic” (Tully and Weber, 2022). Leaked files from the Russia-based ransomware group Conti have shed light on the intricate relationship between these hackers and Russian authorities, hinting at a mutual understanding and even suggesting a chain of command linking Conti to Russian intelligence agencies (Faife, 2022). This revelation has sparked discussions regarding the unspoken guidelines and communication channels that may exist between the Russian government and Conti's leadership (Burgess, 2022). Essentially, Russian cybercriminals appear to operate with a degree of freedom, provided they refrain from targeting Russian interests (Tully and Weber, 2022).

However, these relations can undergo 180-degree changes in the blink of an eye, responding to the political climate. The apprehension of 14 members (8 of them initially charged under Part 2 of Article 187 of the Criminal Code) of the REvil ransomware group by Russian law enforcement in January 2022 seemed to mark an unprecedented moment in the era of ransomware-as-a-service (Recorded Future, 2021). The FSB's official statement confirming these arrests and their focus on REvil appeared to signal a shift in Russia's approach to cybercrime investigations, much to analysts’ surprise (Recorded Future, 2021). Eventually, it became obvious that this move, occurring amid escalating U.S.-Russia tensions prior to the Ukraine conflict, was meant to act more as a diplomatic rapprochement or appeasement to Washington than a crackdown on hackers (Faife, 2022). It seemed to convey that Russia could assist against cybercriminals if the U.S. complied with Moscow's interests in Ukraine (Faife, 2022). Thus, there is speculation that these high-profile arrests may have elements of "signalling," aimed at dispelling suspicions of collusion between cybercriminals and the Russian state, thus enhancing Russia's plausible deniability right before the invasion of Ukraine (Recorded Future, 2021). As the conflict in Ukraine developed, Russia withdrew the charges and purportedly examined the possibility of enlisting the Revil group to join in a way the government’s ranks (Faife, 2022).

Nonetheless, this serves as merely one instance of the sometimes-precarious position of cybercriminals in the hands of the Russian state despite its regular “symbiosis”. According to Canfil, patriotic hackers present a more attractive proposition for state sponsors in the realm of cyber operations (2022). For Canfil, patriotic and ideologically motivated hackers, driven by their political alignment with the state, reduce the need for additional incentives to maintain loyalty and minimise the aforementioned risk. Therefore, it is not uncommon that states delegate specific tasks to these proxies, particularly less sophisticated or sensitive operations (Canfil, 2022).

Within the intricate cyber landscape, relationships between Russian intelligence services and the criminal underground operate under a spectrum of unspoken and explicit agreements, marked by fluidity. Recorded Future has distributed these connections into three distinct categories (2021):

a) Direct associations, which entail specific links between criminal underground actors and state institutions. This encompasses voluntary recruitment by individuals aligning with Russian government interests and coercive recruitment (when apprehended by the government: either prosecution or collaboration with authorities). State-backed underground forums for ad hoc recruitment further exemplify this category.
b) Indirect affiliations, where there are clear indications suggesting the Russian government is leveraging criminal resources or personnel even if direct connections cannot be established. These ties, albeit diffuse, are impactful, supporting Russian government goals through cybercriminal actions. DDoS attacks perpetrated by hacktivists or patriotic hackers would fall under this category. Moreover, Russian intelligence agencies have employed criminal-grade malware to obscure their operations and hinder attribution, and have exploited compromised networks by these hackers to access sensitive data and advance espionage activities (targeting domestic opposition and foreign entities alike).
c) Tacit agreements, which describe overlaps in cybercriminal activities with Russian state strategic objectives. The Russian government allow these groups to conduct their malicious activities but without state involvement. The absence of punitive measures implies a tolerance or tacit approval of these cooperative efforts.

Nevertheless, according to Recorded Future's researchers, "ultimately, whether or not there are connections between Russian authorities and cybercriminals becomes a moot point" since the Russian-speaking cybercriminal community (recognised both domestically and internationally) has faced limited intervention from Russian authorities (2021). And this will likely continue to be the case in the near future.

Following the beginning of the Ukrainian conflict, Russia's cybercriminal landscape has undergone significant shifts. Some criminal groups allied with the state, while others fragmented due to differing ideologies or pursued financial gain amid geopolitical turmoil (Recorded Future, 2023). These changes disrupted underground markets and led to certain "gangs" disappearing (Recorded Future, 2023). Meanwhile, consultancies' reports, like Accenture's, highlight how hacker groups have abandoned traditional norms, with conflict lines dividing them, particularly within the Commonwealth of Independent States (Clarke, 2022). The readmission of ransomware hackers into Russian forums further divides these groups, potentially reshaping from now onwards hacker recruitment based on political causes rather than monetary gain (Clarke, 2022). The incentives are obvious: gain favour with Russian security services, build a relationship offering useful tools and services, and they will provide in return (Recorded Future, 2023).

The difficulty of attribution and other obstacles

Russia's leveraging of plausible deniability remains a problem in attributing these cyberattacks. The Kremlin employs a privateer model, using private criminal hacker groups to obscure its involvement in cyberattacks. It also protects its proxies by exerting great efforts to ensure that its hackers caught abroad are extradited back to Russia (Zilberman, 2018). These employed groups range from the well-known, such as the Wagner Group and the Internet Research Agency, to hackers skilled at hiding their identities and digital presence. Although Russia then denies any involvement, the links between these non-state actors and the Russian government are largely transparent and obvious. The Russian annexation of Crimea in 2014 clearly exemplified this employment of allegedly non-state actors, such as a citizen militia which "lacked any unit markings, but had all the bearing of professional Russian combat forces", which later became colloquially known as the "little green men" (Atwell et al., 2021).

Cyberattacks are often difficult to attribute to a specific actor, even if a plausible suspect can be identified. The question of attribution can be circumvented by focusing on the consequences of the attack, rather than the identity of the attacker. In some cases, it may even be advantageous for the attacker to remain anonymous, as long as this does not undermine the intended effect of the attack (Steiner, 2016). In such cases where the intention is to coerce, the clear communication of threats is complicated greatly by anonymity (Gomez, 2018).

This situation also creates the possibility of false claims of responsibility, which could cause unintended escalation or armed responses. Furthermore, the use of private actors in cyber activities blurs boundaries between public and private. Adequately delineating what degree of control a state would need over an offending non-state actor would constitute a sufficient state attributability remains a challenge (Kastelic, 2022).

Plausible deniability serves different purposes at different levels of politics — internationally, it lets states engage in acts while (ideally) defying repercussions and culpability. Domestically, it allows high-ranking politicians to deny personal knowledge and scapegoat subordinates (Cormac and Aldrich, 2018). Beyond this, the concept of "implausible deniability" blends politics, the military, and covert actions, especially influence operations, with the goal of creating uncertainty about whether a state of war exists and the identification of combatants. The intentional vagueness, aided by Moscow's refusal to acknowledge its actions, allows the Kremlin to gauge international responses and muddles the boundaries between internal unrest and external involvement, and between state and non-state actors. This hinders the global community's ability to distinguish between acceptable and unacceptable behaviour (Cormac and Aldrich, 2018). This ambiguity allows Russia to create its own realities, fuelling myths and scepticism.

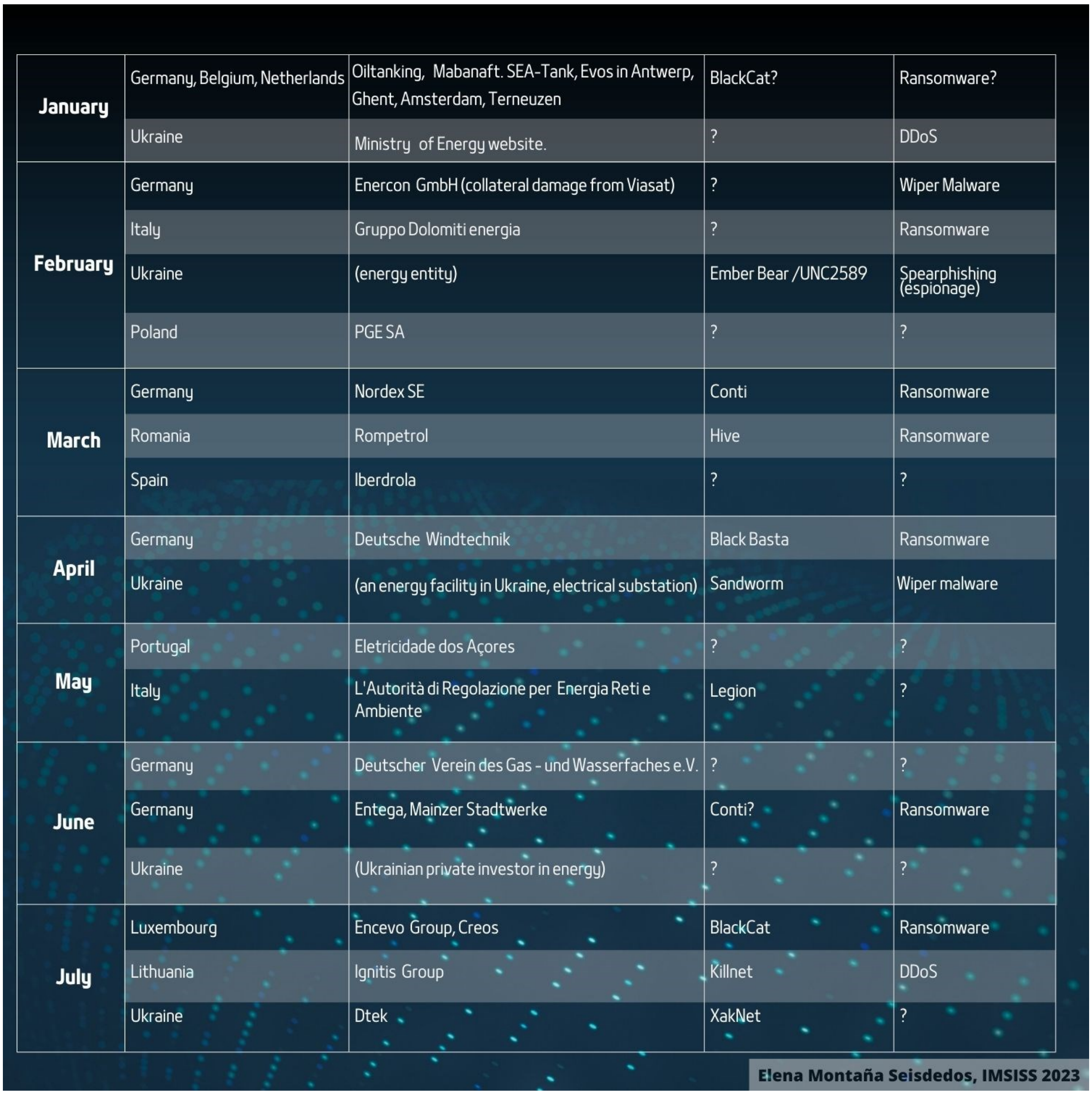
The geopolitics of attribution, while not the primary factor in the process, should not be dismissed. While technical analysis and solid intelligence provide concrete evidence for attribution, a geopolitical assessment helps validate or contextualise the process by considering the attacker's motivation through questions like 'who benefits?' (cui bono) and whether it's a "false flag" operation. Even if an actor claims responsibility, it must be viewed sceptically, as it could be part of a deception strategy. Technical findings, such as the nature of stolen documents and the positions of affected employees, contribute to this assessment. Russia has often been accused of cyberattacks due to its perceived gains from them (Herpig, 2018).

Subsequently, with this in mind, one begins to understand what makes attributing cyberattacks to Russia particularly difficult. In some situations, although initial indices of who perpetrated a cyberattack may point at the Kremlin, too hasty conclusions could lead to misunderstandings or dangerously increased tensions —which is doubly true in scenarios where the relationship is already strained. Political considerations are often influential and taken into account in attributing recent cyberattacks. However, while the UN GGE holds states accountable for cyberattacks carried out from within their territory, offering assistance in investigations can ease suspicion. Furthermore, connecting a cyberattack to a hacker group is different from linking it to a specific state, especially in the context of the UN Charter's requirements for attribution to a particular government or military (Herpig, 2018).

Whereas attribution was historically deemed the “most difficult problem” in cyber operations, recent developments has facilitated this process, making it feasible (albeit laborious). Those targeted can gain insights into the perpetrators and their provenance through using Indicators of Compromise (IOCs) and other technical clues. However, attribution still remains difficult, as those targeted in the private sector may not wish to disclose this, nor disclose IOCs or other sensitive information related to the attack. States will be unlikely to show their hand and disclose what they know about the attacker, as this may help the attacker learn and improve for the future. Regardless, victims increasingly attribute cyberattacks for political reasons, even with limited evidence, as proving state sponsorship is legally challenging. Such state attribution, although unofficial, serves to minimise uncertainty and establishes cybersecurity "truths" for those with the resources to respond or retaliate (Canfil, 2022).

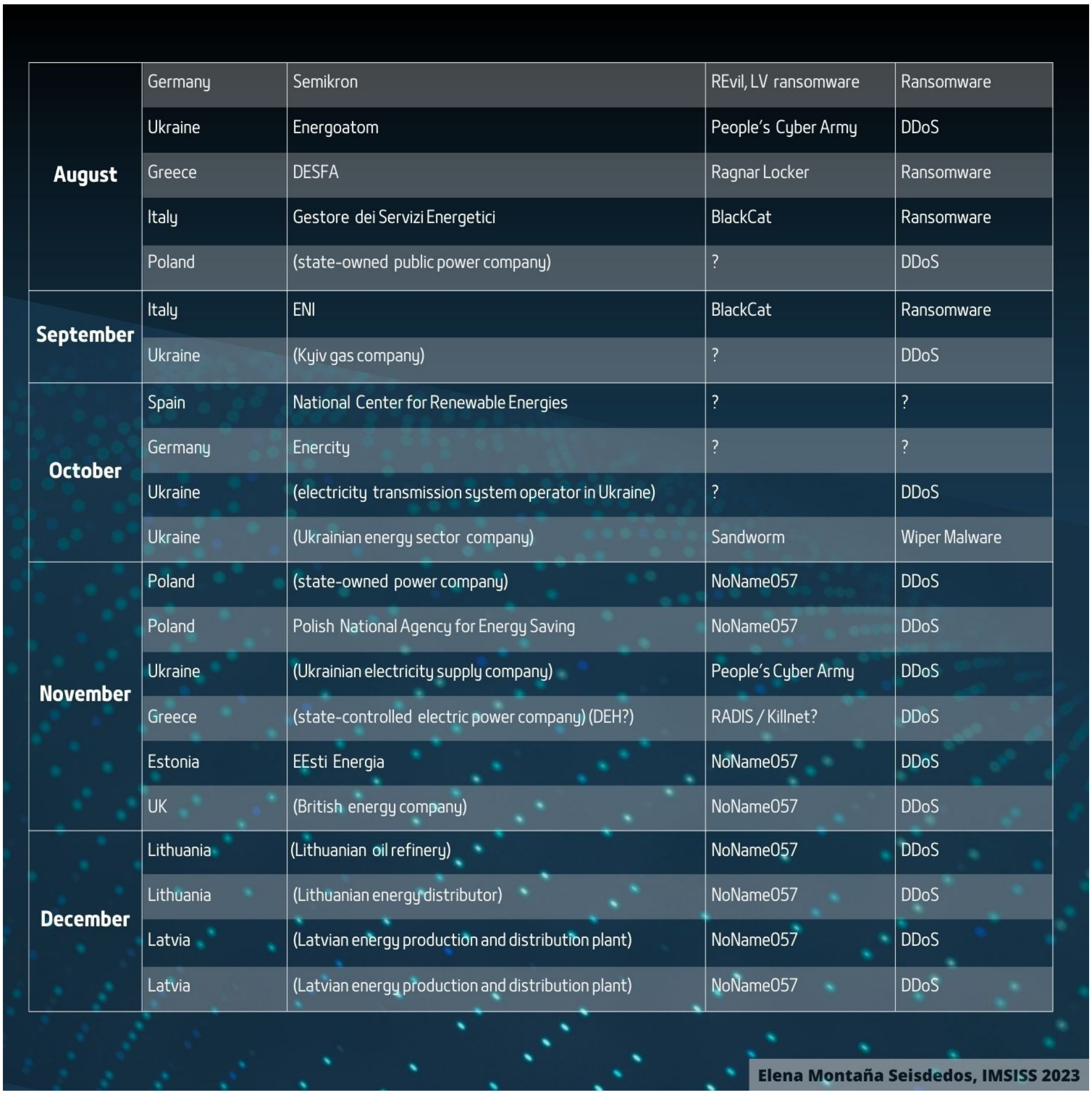
3.3 Study of Cyberattacks Associated with Russia Targeting the Energy Sector in 2022

Summary of attacks in the energy sector by Russian* actors in 2022



January	Germany, Belgium, Netherlands	Oiltanking, Mabanaft. SEA-Tank, Evos in Antwerp, Ghent, Amsterdam, Terneuzen	BlackCat?	Ransomware?
	Ukraine	Ministry of Energy website.	?	DDoS
February	Germany	Enercon GmbH (collateral damage from Viasat)	?	Wiper Malware
	Italy	Gruppo Dolomiti energia	?	Ransomware
	Ukraine	(energy entity)	Ember Bear /UNC2589	Spearphishing (espionage)
	Poland	PGE SA	?	?
March	Germany	Nordex SE	Conti	Ransomware
	Romania	Rompetrol	Hive	Ransomware
	Spain	Iberdrola	?	?
April	Germany	Deutsche Windtechnik	Black Basta	Ransomware
	Ukraine	(an energy facility in Ukraine, electrical substation)	Sandworm	Wiper malware
May	Portugal	Eletricidade dos Açores	?	?
	Italy	L'Autorità di Regolazione per Energia Reti e Ambiente	Legion	?
June	Germany	Deutscher Verein des Gas - und Wasserfaches e.V.	?	?
	Germany	Entega, Mainzer Stadtwerke	Conti?	Ransomware
	Ukraine	(Ukrainian private investor in energy)	?	?
July	Luxembourg	Encevo Group, Creos	BlackCat	Ransomware
	Lithuania	Ignitis Group	Killnet	DDoS
	Ukraine	Dtek	XakNet	?

Elena Montaña Seisdedos, IMSISS 2023



August	Germany	Semikron	REvil, LV ransomware	Ransomware
	Ukraine	Energoatom	People's Cyber Army	DDoS
	Greece	DESFA	Ragnar Locker	Ransomware
	Italy	Gestore dei Servizi Energetici	BlackCat	Ransomware
	Poland	(state-owned public power company)	?	DDoS
September	Italy	ENI	BlackCat	Ransomware
	Ukraine	(Kyiv gas company)	?	DDoS
October	Spain	National Center for Renewable Energies	?	?
	Germany	Enercity	?	?
	Ukraine	(electricity transmission system operator in Ukraine)	?	DDoS
	Ukraine	(Ukrainian energy sector company)	Sandworm	Wiper Malware
November	Poland	(state-owned power company)	NoName057	DDoS
	Poland	Polish National Agency for Energy Saving	NoName057	DDoS
	Ukraine	(Ukrainian electricity supply company)	People's Cyber Army	DDoS
	Greece	(state-controlled electric power company) (DEH?)	RADIS / Killnet?	DDoS
	Estonia	EEsti Energia	NoName057	DDoS
	UK	(British energy company)	NoName057	DDoS
December	Lithuania	(Lithuanian oil refinery)	NoName057	DDoS
	Lithuania	(Lithuanian energy distributor)	NoName057	DDoS
	Latvia	(Latvian energy production and distribution plant)	NoName057	DDoS
	Latvia	(Latvian energy production and distribution plant)	NoName057	DDoS

Elena Montaña Seisdedos, IMSISS 2023

Trends and Patterns 2022

The landscape of cybersecurity has seen notable shifts and developments between 2021 and 2022. Before studying in detail the particularities of the cyberattacks experienced by entities in Europe in a specific period, it is important to acknowledge that cybersecurity as a field is in constant development and as it evolves, so do the tactics employed by malicious actors and the number of distinctive threat groups grow. According to the World Economic Forum's Global Risks Report (2022) the general market trend of escalating cyber threats outpaces the capacity of societies to effectively prevent and manage cyber risks. This alarming phenomenon arises from a confluence of factors.

The ongoing digitalisation of physical supply chains, while enhancing efficiency and connectivity, exposes new vulnerabilities ripe for exploitation by malicious actors (World Economic Forum, 2022). The proliferation of malicious activities is further exacerbated by the burgeoning vulnerabilities in digital infrastructure, compounded by the relatively low barriers to entry for cyber attackers. In this environment, participants can engage in cybercrime with limited risk of extradition, prosecution, or sanction, fostering a sense of impunity. Further aggravating the situation, the cybersecurity landscape is currently hindered by an acute shortage of qualified cybersecurity professionals that could work to counteract these threats effectively. Already between 2019 and 2020, the first years of the pandemic (and lockdowns) that forced the world to undergo a substantial wave of digitalisation, malware increased by 358% and ransomware, more specifically, grew by 435%. Moreover, the past few years have ushered in a new era of aggressiveness and the ubiquity of cyberattacks. Ransomware perpetrators have embraced heightened pressure strategies and are now targeting more susceptible entities, with triple or quadruple extortion of clients and combinations of different types of attacks. The increasing sophistication of cyber tools has empowered threat actors to hone their focus on specific targets, bypassing opportunistic approaches, with subsequent financial, societal and reputational repercussions. At the same time, according to the World Economic Forum, cyber warfare has emerged as a key arena for escalating tensions among global powers, multiplying the risk of substantial disruption of societies' normal functioning and eroding public trust in governmental efficacy or responsiveness to threats (2022).

As explained above, the cyber threat landscape in 2022 was profoundly shaped by the conflict between Russia and Ukraine, and the exacerbation of tensions between European governments and the Kremlin. However, the unfolding of 2022 has seen a remarkable disconnect between projected expectations of cyberattacks and the realities on the ground (whether in Ukraine or the rest of Europe). Cybersecurity analysts and researchers, bracing for the worst, found themselves grappling with a perplexing question: why did Russia's actions not align with their worst fears? The conflict's cyberattack landscape has, thus far, exhibited a level of activity significantly lower than initial forecasts had anticipated. Amidst this apparent respite, cautionary voices have emerged, warning against complacency and a potentially false sense of security. While the current scale of cyberattacks might fall below the envisioned threshold, experts stress the possibility of escalation (Clarke, 2022).

In the months following the onset of the war, analysts have rushed to fill the gaps in understanding, offering insights into the underlying factors shaping the course of events and unravelling the intricacies of why and how this divergence happened. According to Tytler, this is explained by the confluence of both structural and geopolitical factors (2023). These would include the application of sanctions that has heightened global attention on financial flows to Russia and other financial activities, the reduction in major technical vulnerabilities (more due to increased awareness and a boost in cyber defences than an actual reduction of the vulnerability surface), and the possible strategic shift to curtailing some of the previously unrestrained campaigns to avoid retaliatory actions. In fact, we will come to see that Russian cyber activity against Ukraine has been (in comparison to the rest of Europe) highly targeted —governmental and private entities alike have experienced DDOS attacks, website defacements, phishing campaigns, wiper attacks, and other forms of malware deployment (Recorded Future, 2023. Tytler also believes that cybercriminals like ransomware groups might have adjusted their focus and toned down their attacks influenced by Kremlin's directives (2023). For others, Russian cyberattacks have just failed to achieve their intended goal and impact (Pascual, 2023).

Analysts are split between those who argue that the Kremlin's cyber capabilities have been overestimated and those who contend that Moscow is yet to deploy its full cyber power for strategic reasons. According to Daniel Moore, Russia's actions align with expectations in the sense that it has employed cyberattacks alongside military actions to hamper Ukrainian communications, but Russia’s technical prowess is hindered by operational disorganisation (Pascal, 2023). He also believes that the Kremlin’s cybersecurity efforts have been overshadowed by its disinformation campaigns (Pascal, 2023). Carnegie analysts believe that the problem was Russia overestimating its capacity to maintain cyberattacks against other countries as the war raged on, and “not fully leveraging cyber criminals as an auxiliary force against Ukraine” (Bateman et al., 2022). They also suggest, —similarly to Moore— that cyber operations tend to be more “impactful and resonant” in periods of relative peace than during a conflict characterised by “violence and destruction”, and that they are probably curtailed given the possibility of a clash with NATO (Bateman et al., 2022). It is also suggested that the limited experimentation and targeted operations against Ukraine’s allies might be explained instead by Moscow’s focus on gathering valuable intelligence to leverage vis-à-vis Ukraine and in Russia’s interaction with other countries.

Nonetheless, the conflict has also birthed new phenomena. According to analysts at Sekoia, “moving away from the traditional model of unstructured and decentralised collectives, [we are] witnessing the emergence of hierarchical groups, aligned with political agendas, possibly supported by State-nexus resources, and capable of conducting large-scale coordinated campaigns” (Tibirna and B., 2023). In 2022, the number of attacks reached an unprecedented peak (James, 2023), with a notable 150% surge in ransomware attacks, leading to damage even in robust and well-established markets (Klimburg, 2022).

According to Thale~~’~~s’ Cyber Threat Intelligence Unit (2023), the most relevant shift occurred in the third quarter of 2022, transitioning from a Ukraine focus to wider (and intensified) cyber warfare spanning across Europe. While the majority of incidents were initially confined to Ukraine (50.4% in the first quarter of 2022 compared to 28.6% in the third quarter), from the third quarter of 2022 EU nations witnessed a significant surge in conflict-related incidents (9.8% to 46.5% of global attacks). By the summer of 2022, EU countries experienced almost as many conflict-related incidents as Ukraine itself. The European Union has seen the majority of incidents (80.9%) in the first quarter of 2023. The third quarter of 2022 also represented a shift toward DDoS attacks, which became the favoured method (75%) by cyber attackers against both companies and governments, with a subsequent increase in the latter part of the year. Notably, destructive cyber-military operations and espionage accounted for a mere 2% of total incidents, primarily targeting Ukrainian public-sector organisations (Thales, 2023).

The energy sector mirrored this general trend. In the third quarter, cyberattacks on energy and commodities infrastructure surged significantly, setting a record high for major incidents reported within a year, as highlighted by the update from S&P Global Energy Security Sentinel (James, 2023). This rise in cyber threats aligns with the heightened tensions between European nations and the Russian Federation over energy issues, prompting cybersecurity experts to anticipate the energy sector as a prime target for destructive cyber operations aimed at European and Ukrainian entities. This projection is reminiscent of previous cyber campaigns, such as those supporting the annexation of Crimea in 2014, which also underscored the strategic significance of energy. The war and its global implications for energy supply played a role in driving malicious cyber activities, coming from both “State-nexus threats” and hacktivist groups (Tibirna and B., 2023). Researchers have identified Russia-linked intrusion sets engaging in destructive and disruptive cyber campaigns targeting the energy sector, with encompassed a wide range of offensive cyber operations (such as espionage, sabotage, and information warfare). At the same time, hacktivists displayed an increasing inclination towards disruption operations targeting energy entities, scaling up DDoS attacks, data disclosures and defacement operations. Furthermore, the European energy sector experienced a surge in cyber malicious campaigns, particularly lucrative-oriented double extortion attacks orchestrated by Ransomware-as-a-Service (RaaS) groups, along with hack-and-leak operations. MSTIC reported that Russia-nexus intrusion sets' campaigns targeting the Ukrainian energy sector and nuclear-related entities accounted for 8% and 3% respectively of State-nexus activities originating from Russia in 2022 (Microsoft Threat Intelligence Center, 2023).[6] According to researchers at Sekoia, the year also witnessed the identification of 34 instances of ransomware groups conducting malicious campaigns against the energy sector in Europe, a notable increase from the 30 known attacks in 2021 (Tibirna and B., 2023). These incidents encompassed various segments of the energy sector: electricity supply and distribution, generation, specialised professional services, storage, transportation of energy products, oil and gas services, logistics, and renewable energy solutions.[7] These researchers indicate, however, that ransomware activities in this sector are of a highly opportunistic nature, leveraging the criticality of the sector (Tibirna and B., 2023) and the current state of (geo)political affairs.

Strategic Outlook

The energy sector as a target

Among the diverse array of potential targets for cyberattacks, one particular sector stands out for its criticality and its centrality in Europe-Russia relations: energy. This section raises a fundamental question: why would hackers, whether acting on behalf of state-sponsored efforts or independent malicious actors, direct their attention toward the disruption of energy? As we delve into the intricate landscape of cyber threats, it becomes imperative to explore the motives, vulnerabilities, and potential repercussions that make the energy sector an attractive focal point for cyber operations.

Scholars assert that the most expedient way to undermine a nation's resolve is by targeting its economic foundation through precision attacks, aiming to weaken its very existence —and that would be the energy sector (Aljohani, 2022). The energy sector is crucial to a nation's economic and industrial activities. Shakeel (2022) highlights precisely this point, that the energy sector's vulnerability is exacerbated by its interconnection with numerous

[6] The reports from Microsoft regarding the war in Ukraine have ignited criticism among cybersecurity experts and foreign policy scholars, who believe that Microsoft might be attempting to shape the state of the conflict's cyber realm in Ukraine to "further its commercial interests". See Smalley, 2022. (https://cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/) -- If this was true and extended to cybersecurity/technology companies alike, most information made public and available online outside of traditional media platforms and think tanks (whose information often is lacking in detail and abundant in inaccuracies) could not be deemed reliable.

[7] The energy sector includes oil and gas companies, alternative energy producers, suppliers and utility providers. It spans three categories: "a) the exploration, production and refinery of energy; b) the marketing, storage, distribution and transportation of energy; and c) the delivery of energy equipment and services" (Allcot, 2021).

industries and society at large, serving as the driving force behind industrial, technological, and administrative processes. Taking this into account, it is not surprising that hackers want to exploit the opportunity to disrupt the energy supply of a nation, threatening to cripple its everyday functions. In 2019, for instance, according to the U.S. Department of Energy, hackers breached the web portal firewall of a solar power utility, resulting in operators losing visibility for parts of the grid for 10 hours. As a more extreme example, a mere six-hour power outage in a country like France could incur damages exceeding EUR 1.5 billion (James, 2023)[8].

The energy sector has unique interdependencies between physical and cyber infrastructure (IT and OT) which could lead to physical destruction. It has very specific vulnerabilities, stemming from factors such as its expansive attack surface —given the geographic and organisational complexity, with multiple suppliers, providers and producers involved[9]— , the scarcity of skilled cybersecurity professionals, and the challenges brought about by digitalisation, integration and increased automation. The energy sector has embraced digital transformation relatively late and this has left it globally deficient in cybersecurity expertise and maturity, according to James (2023).

As outlined above, given their essential role, energy companies also constitute an attractive target for those looking at the prospect of financial gain, as they cannot afford downtimes in their operations and are more likely to pay for any ransom. A telling example, despite taking place in the U.S., is the case of DarkSide's 2021 hack of Colonial Pipeline, which led the company to shut down the pipeline and, amid the ensuing panic among Americans, pay off an over 4 million dollar (USD) ransom (Kerner, 2022). The incident led to shortages that spiked prices of oil momentarily —impacting for instance the functioning of several airports—, and declarations of emergency in several states (Sabin, 2023). The ransomware gang did not have access to the whole system, but the company was forced to stop operations as a precaution to prevent the malware from spreading.

According to Ferris, "concerns long pre-date the current crisis" and the war in Ukraine, albeit now heightened (2022). Vulnerabilities are likely to increase with the energy sector transitioning towards net zero carbon emissions, expanding the use of renewable sources and the progressive digitalisation of supply networks. This will imply greater dependency on electricity (as opposed to fossil fuels), with a decentralised electricity generation model, making energy systems more accessible and broadening the spectrum of potential targets of hackers (Ferris, 2022). Cybersecurity experts like Jesper Olsen, have also pointed out that there is a correlation between the worsening state of the economy and the increasing aggressiveness of threat actors (Carter, 2023). Moreover, there is an apparent financial interest among threat groups in supporting Russia, provided the state will also have their backs: "those that are already pro-Russian, they would like to engage more with and support them in terms of this conflict" (Carter, 2023).

[8] More creative scenarios involve tampering with electricity meters, taking advantage of 2022-2023's high energy prices (Dawda, cited by Ferris, 2022) See: https://www.newstatesman.com/spotlight/sustainability/energy/2022/05/the-hackers-out-for-energy

[9] According to a report by the World Economic Forum, energy cybersecurity becomes fraught with challenges, particularly since "cyber hygiene is siloed and responsibility shared across diverse priorities" (Klimburg et al., 2022).

Energy cyberattacks as a tool of economic warfare

It has been argued throughout this dissertation that cyberattacks can in fact be utilised as a tool of economic warfare provided that it meets certain criteria. One of the conditions it should meet is that the attacks —whether in singular or as a whole— have to target or aim to impact the economy of a state, ensuring coercion through geoeconomic instruments. Given the abovementioned centrality of the energy sector within national economies, it is appropriate to consider to what extent energy-related cyberattacks could hinder said economies —beyond national security concerns. As a reference point, we should take into account that cybercrime is estimated to have a cost of 10.25 trillion USD globally by 2025. However, on a company level, one encounters multiple obstacles to calculating the impact of cyberthreats: there are both tangible and more abstract costs (Smolanoff and Greene, 2023). These encompass, on a general level, direct financial losses (due to operational downtime) and immediate costs (ransomware payments, for example), investigation and repair/recovery costs (Smolanoff and Greene, 2023), and potential disruption to various industries heavily reliant on consistent energy supply and other associated activities.

Moreover, cyber incidents erode public trust in the company, and can even prompt regulatory changes —as was the case with Colonial Pipeline— and increased compliance costs —the average cost for entities facing non-compliance issues is $14.82 million and in 2021, GDPR fines totalled $1 billion (Smolanoff and Greene, 2023)—. Additionally, the ripple effects of cyberattacks can undermine productivity and influence investment decisions. This highlights the intricate interplay between cybersecurity, the energy industry, and the overall economy.

Kroll's CFO research also highlighted other (less obvious) consequences:

- 7/10 companies studied lost 5% or more of their valuation after their biggest cybersecurity incident in the 18 months before the research.
- The average returns after the attack for the companies studied were -0.65%, whereas the average return the year before was +8.47%
- The cost of increased cybersecurity investment after the attack as well as the loss of market value can be transferred to customers through higher prices (leading to inflation) or their reduced income might translate into lower investment, lower employment and reduced growth.

According to another source, Morningstar Sustainalytics, an important cyberattack has an impact on a company's stock price for a longer period than one would expect (50 trading days) (Zerter and Hudson, 2022) and companies that suffered cyber incidents also considerably lag the market and sector benchmark in the year after the attack.

In the specific case of energy companies, direct costs referred to those absorbed directly by providers or owners, like repairing damaged networks or any other element. But there are also losses suffered by the users of its infrastructure that are also impacted more indirectly by the attacks and are not responsible for the maintenance of the critical infrastructure systems (Piotr and Jacob, 2019). And concerning Russia, economists claim that the country is responsible for two-thirds of the 1 trillion USD global annual economic damage caused by cyberattacks (Kennedy, 2022). This should be computed together with the already difficult situation faced by European energy markets in 2022, with unseen peaks in prices and low oil/gas inventories (Klimburg et al., 2022)

Even often-dismissed DDoS can represent an important challenge. While many people associate DDoS attacks with their original volumetric tactic, these threats have evolved (Deamer, 2018). Hackers now employ them as a precursor to launching more intricate attacks. Most DDoS attempts are relatively small, under 10Gbps in volume, last less than ten minutes, and can go unnoticed by IT security teams (Deamer, 2018). Hackers can later infiltrate networks and deploy malware or engage in data theft, leading to the aforementioned list of incurred costs like the interruption of business operations, penalties, fines etc (Deamer, 2018).

Analysis of the sample

Per type of attack

The analysis presented in this dissertation delves into the most pertinent cyberattacks documented across various sources, including media websites, publications from cybersecurity firms, and other reports tracking cyberattacks throughout the year 2022 (whether it is separated per sector or the ‘energy element’ has been identified manually). This research aims to provide a reflection of reality within the constraints of available free and open sources. While the number of attacks studied here may be fewer than the total incidents experienced by European companies and institutions related to the energy sector, the selected cases are significant enough to have garnered media attention or inclusion in reports by reputable cybersecurity firms, thereby capturing pertinent trends.

Problematically, energy is referred to both as critical infrastructure and a critical sector in some media outlets, with both terms used as if they were interchangeable. This introduces new complexities in distinguishing the impact and attacks on energy sector companies from those on public institutions dedicated or focused on this sector, as well as the utilities themselves. Regrettably, the distinction is particularly crucial for accurately assessing the extent of damage caused by cyberattacks. The evaluation of wiper malware operations against Ukraine poses an additional challenge, as the reporting standards and practices vary greatly between sources, leaving the differentiation between “attempts” and “successes” unclear. This situation necessitated extensive cross-referencing among sources and generated uncertainties regarding the comparability of all types of attacks (ransomware, DDoS…) included in the sample. This is added to divergences in dates (months) reported by think tanks and cybersecurity companies, an issue that might be rooted in the existence of various stages within the same operation, in the fact that the operations were discovered much later after they had been launched, or because the incident is made public sometime after the cyberattack actually was initiated and discovered. On a more general level, naming has also constituted a problem on various occasions, with threat actors being called multiple names (and numbers) by different researchers or some attacks being registered with no more specification than “energy utility from country X targeted by Russian hackers”. There is often no mention of the type of attack nor of a particular hacking group.

Despite these challenges, the collection of cyberattacks attached in this document strives to provide a comprehensive (although perhaps slightly inaccurate/inexhaustive) portrayal of the evolving energy cyber threat landscape in Europe. It draws from credible and diverse sources to present an informed and nuanced understanding of the observed events, as well as the diversity of actors connected to Russia. Lastly, a disclaimer must be included regarding the threat actors included in this list. All the hacking groups presented in this document have been associated in one way or another with Russia, but this is not to say that they are all of Russian nationality or that they are all a subset of the Russian state apparatus (particularly Russian intelligence services) or managed by/in communication with the Russian state.

The scope of the analysed cyberattacks encompasses a total of 40 distinct cases. This sample spans four diverse categories of attacks or operations, namely ransomware, Distributed Denial of Service (DDoS), cyber espionage, and wiper malware. Notably, ransomware attacks featured consistently in 2022, accounting for 11 out of the 40 cases under scrutiny. The prevalence of DDoS attacks was evident as well, constituting 17 out of the 40 cyberattacks. Wiper malware attacks were documented in 3 out of the 40 cases, and a single spearphishing attack was identified as potentially linked to a broader cyberespionage campaign. In addition to the aforementioned cases, while not explicitly included in the table above, in the period between December 2021 and March 2022, the Dragonfly (BROMINE) hacking group was observed engaging in data exfiltration from a nuclear safety organisation. The group is known for its espionage operations, showing interest in energy and is affiliated with Russia. Similarly, the Gamaredon APT (Primitive Bear) group undertook a targeted operation against a NATO petroleum refining company in August 2022, albeit unsuccessfully.

For the purposes of this dissertation, ransomware will be considered (following the typology presented in the theoretical framework) as a disruptive cyberattack. Of particular relevance due to the damages observed is the January BlackCat ransomware attack, which reportedly affected hundreds of petrol stations in northern Germany (Greig, 2022). Oiltanking supplied fuel to 26 companies in the country which operate thousands of petrol stations. Although the fuel supply remained unaffected by the attack, the repercussions were substantial, since the attack incapacitated essential IT systems that managed the automation of tank loading and unloading procedures, a task that is not feasible to carry out manually. Consequently, the 13 tank farms under Oiltanking's purview were unable to accommodate trucks, necessitating the utilisation of alternative approaches (Greig, 2022). Oiltanking invoked a “force majeure” clause for a significant portion of its German supply citing that a “catastrophic event” beyond its control hindered the company’s contractual obligations (Glover, 2022). Mabanaft Deutschland GmbH & Co also invoked “force majeure” and, outside of Germany, difficulties were encountered in the unloading and loading of refined product cargoes by a minimum of six oil storage terminals within the Amsterdam-Rotterdam-Antwerp refining hub. Dutch oil and gas storage company Evos was also hit by the attack.

This development did not escape the attention of international analysts, as it holds potential implications for Europe’s energy supply. Notably, approximately one-third of Germany's oil and gas was sourced at the time from Russia through Nordstream 2, accentuating concerns that a cyberattack causing disruptions could intensify Germany's dependence on the mentioned pipeline (Glover, 2022). Statistics from the months following the attack show that Germany is a particularly distinct target for ransomware, the most attacked country in the EU and the fourth most attacked globally by known attacks (Malwarebytes Labs, 2023).

Ransomware attacks have a relatively high impact on organisations and their supply chains, as higher costs are inflicted upon these entities in comparison to other types of attacks. However, sophistication (and the level of damage of attacks) varies with a multiplicity of options available to hackers through RaaS (Ransomware as a Service), which allows affiliates to pay to launch attacks without the need of developing the malware themselves (renting or purchasing the capacity to inflict considerable harm). According to Jun (2021), analysts and scholars concur that achieving coercion in cyberspace is quite difficult, but ransomware could be an exception. For Jun, ransomware (extortion through encryption and leaks) has demonstrated its ability to effectively extort victims due to Russia's provision of safe havens for cybercriminals and has shown superior efficacy in “hostage-taking” compared to conventional methods like blockades (Jun, 2021). The encryption of a target's data serves as a definitive credible signal of the attacker's capability and allows attackers to impose costs on victims automatically while avoiding incurring costs themselves. Moreover, its reversibility adds an extra incentive for victims to comply. On a larger scale, the conditional denial of economic activity by holding data hostage can threaten economic prosperity in the information/digital era and bear geopolitical implications (Jun, 2021).

Of the cyberattacks tracked for the purposes of this dissertation, Denial of Service attacks (another form of disruptive attack) represented a large percentage. In 2022, DDoS attacks increased in the months following July, becoming extremely present in November and December. These attacks comparatively had a lower impact on their targets and are characterised by lower sophistication. While it has not been made public to what extent these DDoS attacks impacted the activity of the energy entities found in the table above, the reader can refer back to Deamer’s (2018) analysis of the impact of this type of attack in a general manner beyond the immediate loss of revenue, loss of customers, reputational impact, and the cost of service restoration and added cybersecurity measures. An average DDoS attack, according to a 2020 NETSCOUT report, has an average cost of 221,863 USD, although certain attacks can cost victims millions of dollars (Frackiewicz, 2023). This being said, its political significance when launched at the right time can be far superior, driving tensions. According to Kaspersky, already in the first quarter of 2022 the world witnessed “an all-time high number of DDoS attacks” influenced by the geopolitical situation and “some of the attacks observed lasted for days and even weeks, suggesting that they might have been conducted by ideologically motivated cyberactivists” (2022). These types of attacks were also identified during Russia’s conflict with Georgia in 2008 and in 2007 among increasing tensions with Estonia, but to a lower extent.

However, the cyberattacks that received the most international attention were wiper malware attacks launched by APT groups with a clear focus on damaging (rather than disrupting) the targets and destroying data. It is not coincidental that most of these operations specifically targeted Ukraine, while there were probably many more attempts that have not been recorded in the sample of this dissertation. In fact, cybersecurity firms have confirmed that, in 2022, Ukraine suffered more wiper malware than “anywhere ever”, with Fortinet counting “16 different families of wiper malware” throughout the year in Ukraine (Greenberg, 2023). These attacks were, in comparison to the other attacks tracked, more sophisticated. Nonetheless, it has been said that cyberattacks targeting Ukraine in 2022 have consisted mostly of "quick, dirty, relentless, repeated, and relatively simple acts of sabotage", prioritising quantity over quality in terms of its wiper code (Greenberg, 2023).

The most impactful wiper malware attack touched on the energy sector through the Viasat satellite (aiming to halt Ukraine's military communications), disrupting wind turbines in Germany. Other wiper malware attacks targeting the Ukrainian power grid (April) or energy companies (October) were stopped before hackers managed to take down the energy systems as planned. While the first attack described seemed to reuse existing malware, the October attack employed a wiper unknown until that moment and was further accompanied by the launching of missile strikes targeting other Ukrainian energy infrastructure (ESET, 2023). Notwithstanding, the April attack on the Ukrainian energy provider that powered electrical substations led to a station losing power for an hour. Moreover, the attack of Ukrainian energy company DTEK in July also could have been coordinated with the shelling of the Kryvoriska thermal power plant (owned by the same company), which leads researchers to believe in some degree of organisation or similarity of goals between hackers and Russian military forces (Rohner, 2023). Unfortunately, not much has been disclosed about the impact or scope of these cyberattacks, but the most important cyberattacks across the globe in the past two decades have actually been/involved wiper malware attacks —Saudi Aramco in 2012, Ukraine in 2017 etc.

Lastly, at least one cyber espionage campaign was identified targeting a Ukrainian energy entity, with an additional operation (not included in the table) discovered in 2022 (active since 2019) targeting renewable energy and industrial technology organisations from 15 entities globally (Toulas, 2022), among which can be found European companies such as: Schneider Electric (French), CEZ Electro and the Hardzhali Hydroelectric Power Station (Bulgarian). According to reports, "evidence points to two clusters of activity, one from APT28", a group with links to the Russian state also known as FancyBear (Toulas, 2022).

Per target

Analysing the targets (countries and entities) of cyberattacks provides valuable insights into the underlying motivations of the perpetrators, particularly in the context of state-sponsored or state-aligned cyber actors. The selection of victims is closely intertwined with the intended scope of damage caused by the cyber assault. Notably, the nation most frequently targeted is Ukraine, accounting for ten out of the forty analysed attacks, followed by Germany with eight instances. The Baltic countries collectively rank as the third most targeted region, while both Italy and Poland have each experienced four attacks out of the forty examined. This data, when combined with insights from other analysts, suggests a correlation with the escalating tensions between Russia and the affected countries, especially those that have shown support for Ukraine during the conflict. Beyond mere attack frequency, it is equally important to underscore the distinct types of attacks faced by each country or region. This divergence becomes particularly pronounced when contrasting Ukraine's experiences with those of other European nations. Attacks against Ukraine were highly targeted and of varied nature (including DDoS and different wiper malware attacks). It is not only the total number of attacks which stands out, but the motivation transpired by the sophistication and type of the attacks, which answers more to infiltration and degradative attempts.

The attacks for the rest appear to be closely tied to each country's relations with Russia, with varying degrees of energy dependency, proximity to the conflict in Ukraine, and their stance on the war playing significant roles. Germany found itself mainly targeted by ransomware groups (on five occasions). According to Thales, Germany suffered 58 important cyber incidents in 2022, in stark contrast with other European countries that have been relatively spared, like France, the UK or Spain (2023). Italy’s various energy entities were also targeted on three occasions by ransomware, while the country was also a victim of hacktivism. Lithuania, Latvia, and Estonia collectively were targeted by six out of forty energy sector cyberattacks according to the sample, with all of them being DDoS attacks. These cyberattacks were mostly concentrated in the last two months of 2022. While DDoS are often deemed less worrisome than other types of operations, Lithuania described the attack against Ignitis as the most significant in the last ten years, and Estonia received a number of cyberattacks unseen since 2007. Moreover, Thales reports indicate that there have been 157 incidents in total registered in the three countries in 2022 (2023). Ultimately, Poland’s energy sector was also targeted mainly by DDoS attacks, registering 114 cyber incidents (including other sectors) in connection with the Ukrainian in 2022 (Thales, 2023).

A common thread among these targeted countries is their extensive support for Ukraine, both in terms of military aid and economic contributions. This support has escalated their tensions with Russia and heightened their security concerns (leading to increased investment in defence), potentially creating a security dilemma. Additionally, these nations have made concerted efforts to reduce their large dependence on Russian fossil fuels, aiming for energy independence. This shift in energy relations could be seen as an affront to Russia and a motivation for cyberattacks aimed at disrupting their progress, punishing them for their progressive but clear attempt at decoupling from Russia or sending a message of disapproval for their stance towards the war. Likewise, Bulgaria's vulnerability to cyber espionage (mentioned in passing above, although it is not included in the sample) can be attributed to its significant import of Russian natural gas and opposition to Russia’s actions in Ukraine, creating a logical basis for the operation. As laid out in the context chapter above, there are more than enough reasons for Russia’s resort to coercion in its relations with these countries.

If we focus our analysis instead on more generic factors, like the significance of these countries' economies and their populations (what threat actors tend to focus on according to Sussman and Mok, 2023) we obtain few more answers to the question of ‘why me, dear god?’. These factors could be a plausible explanation for attacks against German energy entities (with a population of around 83 million) or Italian energy institutions and companies (with approximately 60 million people), but they offer weak grounds to back the attacks targeting the Baltics. Despite their technological prowess, the Baltics collectively have a population that is 7% of Germany’s (almost 6 million). Comparatively, it is more likely that cyber operations are rooted in the previous reasons, and fuelled by the resentment of Russia losing its grip over its former Soviet circle of influence. Russia is sending a message, as it aims to deter others from doing the same.

Per hacking group

Hacking groups targeting the European energy sector in 2022 can be divided in a general manner into three broad categories: hacktivists, cybercriminals, and APTs. According to Thales, hacktivist groups with pro-Russian affiliations accounted for a significant 61% of reported cyberattacks since the conflict's onset (2023). This statistic highlights the prevalence of hacktivist involvement also observed in the analysis of the 2022 sample. Hacktivists are individuals or groups who use hacking techniques to express their social, political, or ideological beliefs… in this case, showing support for the Russian cause and narrative through disrupting digital systems and networks. Through the months multiple hacking groups have made their appearance, with NoName057 being responsible for 8 out of 17 DDoS attacks, People's Cyber Army committing 2 of those 17 DDoS attacks, and Killnet and XakNet the remaining 3 (2 and 1 respectively).

There was also an abundance of ransomware groups. BlackCat, for instance, was linked to a significant portion of the ransomware attacks observed in 2022. While ransomware gangs such as BlackCat, Black Basta, Conti, and REvil are often thought to focus primarily on obtaining financial rewards for their operations, their numerous ties to Russia raise suspicions of state-level coordination or endorsement by the Kremlin.

Lastly, with a more obvious connection to the Russian state, Advanced Persistent Threat (APT) groups including Sandworm and Ember Bear, played a role in 4 out of the 40 attacks studied. The wiper malware attack that through Viasat affected the German company Enercon GmbH was attributed by the Five Eyes to the Russian GRU without further details. APT groups are perpetrators of a wide array of attacks, capable of conducting cyber operations to (a) influence political events, policy outcomes or public opinion through means like disinformation,(b) steal valuable intellectual property and sensitive data, (c) to gather intelligence from organisations linked to adversaries of the Russian state, (d) to assert dominance and gain military advantage in a conflict, (e)to sabotage critical infrastructure and essential services and, ultimately, (f) coerce other countries into changing their positioning vis-à-vis Russia. These goals, however, are not mutually exclusive since the motivations of these groups are changing and multifaceted. They vary according to the interests and priorities of the sponsoring state. The case of the Cuba ransomware illustrates this reality, as researchers describe that while the group appeared initially financially motivated, it ended up switching to conducting intelligence-collection operations and deploying malware on government systems (Greig, 2023).

Strategically, Russia leverages its Advanced Persistent Threats (APTs) to infiltrate critical infrastructure, with the aim of securing the capacity to disrupt energy supplies during periods of conflict (Sueur and Juijkx, 2022). This manoeuvre serves a dual purpose: incapacitating potential adversaries and deterring them from initiating significant hostilities (Sueur and Juijkx, 2022). Their techniques allowing them to get there are changing. Russian APT groups such as UAC-0113 have utilised easily accessible malware in 2022 from Russian-language forums and incorporated ransomware-like tactics to obscure their use of custom destructive tools. The objective would be, on the one hand, complicating attribution efforts (increasing Russia's plausible deniability power), and on the other, reducing the costs of espionage campaigns, as indicated by Recorded Future's analysis of Russian APT behaviour (Recorded Future, 2021).

There are mainly two APT actors delineated within the 2022 dataset. Ember Bear (UNC2589, Frozenvista), accredited with a spear phishing campaign targeting individuals affiliated with a Ukrainian energy entity, exhibits a propensity for weaponising acquired access and data from infiltrations to bolster their information warfare endeavours (Crowdstrike, 2022). Crowdstrike's assessment attributes this entity to the Russian GRU with a level of moderate confidence, primarily stemming from its Tactics, Techniques, and Procedures (TTPs). It is noteworthy that Ember Bear's affiliations, in contrast to other threat actors, exhibit less conspicuous associations with specific Russian services, and do not exhibit discernible ties to previously tracked adversaries (Crowdstrike, 2022). More proliferate than Ember Bear is the group Sandworm or Voodoo Bear, which has been associated with the GRU Unit 74455. The Sandworm cyber threat group has been consistently engaged in a series of targeted actions within the energy sector, focusing particularly on hack and leak operations, a pattern notably sustained throughout the duration of the conflict in Ukraine. According to Ribeiro (2023), this group is widely suspected to have affiliations with 'CyberArmyofRussia' or 'CyberArmyofRussia_Reborn'. Renowned for their multifaceted capabilities and strategic targets that align with sectors of strategic significance for Russia, Sandworm, as emphasised by Google’s TAG, is recognised as one of the most versatile cyber actors operating under the GRU umbrella (Greig, 2023). Sandworm's track record encompasses an array of high-profile incidents, including the infamous December 2015 cyberattack on Ukraine's power grid, the 2017 deployment of the NotPetya malware, spear phishing attacks during the 2018 Winter Olympics, as well as reconnaissance and hacking attempts directed towards the Parliament of Georgia (Greig, 2023). This has earned the group a reputation for highly destructive capabilities.

Ransomware groups, including LockBit, BlackCat, RagnarLocker, Cuba, and Hive, emerged in 2022 as active cyber gangs significantly interested in the energy sector (Tibirna, 2023). Analysts routinely scrutinise their operations, drawing attention to their potential connections to the Russian state (Tibirna, 2023). One such group, BlackCat Ransomware publicly declared its apolitical stance regarding the Russian invasion of Ukraine in February 2022, distancing itself from the pro-Russian position taken, for instance, by the Conti Gang (Recorded Future, 2023). While there is no clear evidence linking their attacks to the Russo-Ukrainian conflict or the worsening tensions per se, the Russian-speaking affiliates, the timing of the attacks and the resulting circumstances (the disruption and the economic impact) have led researchers to link the two. More politically involved was the Conti Ransomware group, albeit explicitly only temporarily. Conti initially expressed support for the Russian government's actions in the war but later revised its stance (although they condemned cyberattacks against Russia). The group posted an initial statement warning that they would use “all possible resources to strike back at the critical infrastructures of an enemy [of Russia]”, later refined into an announcement of their “full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia and Russian-speaking region of the world” (Recorded Future, 2023). However, Conti later clarified that, although hard to believe, it did not ally with any government.

Other groups (not present in the table) like the LockBit 2.0 ransomware-as-a-service group also affirmed their supposed apolitical nature (Recorded Future, 2023). Unfortunately, in the case of RagnarLocker, there is virtually no information regarding its connection to the Russian state, but it is telling that the ransomware group avoid including among its targets the member of the Commonwealth of Independent States formerly integrated into the Soviet Union (Wadhwani, 2022). This group is particularly specialised in targeting energy and other critical infrastructure organisations according to the experts, which boosts threat perceptions. But there could also be more nefarious goals behind the mask of profit-seeking cybercriminal gangs (Wadhwani, 2022).

However, as it was indicated before, it is hacktivists that have gathered the most attention in 2022. Hacktivists' activities directed towards the energy sector are primarily intended to erode public confidence in the ability of governments and companies to safeguard crucial systems, ultimately weakening support for involved parties through media portrayal of their actions (Tibirna, 2023). These hacktivist efforts don't aim for sustained disruption but rather seek widespread impact by targeting symbolic and vital sectors like government, energy, and telecommunications, driven by ideological motivations (Tibirna, 2023). According to Recorded Future, In the wake of the conflict's onset, two pro-Russian hacktivist groups, Killnet and Xaknet, emerged as vocal supporters of the Kremlin, working under the umbrella of the Cyber Army of Russia (2023). The Cyber Army of Russia is a powerful source of disinformation, but it also orchestrates propaganda efforts for Killnet and Xaknet, which at the same time work jointly by coordinating attacks against perceived adversaries of Russia (Recorded Future, 2023).

The Killnet hacktivist group has attracted substantial attention and intrigue within the realm of cyber campaigns, particularly for its vigorous targeting of Ukrainian and NATO entities, underscored by its unabashed pro-Russian orientation (Recorded Future, 2023). While a nuanced evaluation of Killnet's capabilities yields diverse perspectives, there is a certain consensus acknowledging its status as a notable disruptor within the hacktivist landscape since it first emerged in March 2022. The group's repertoire encompasses a multifaceted approach, encompassing various tactics such as DDoS attacks, hack-and-leak operations, and the defacement of websites, all adeptly designed to bolster and propagate a compelling pro-Russian narrative (Avertium, 2022). However, some question the portrayal of the group as a highly dangerous collective. These cautionary voices explain that the group is far from representing the threat of more highly skilled groups (mainly APTs), does not develop custom tools, and their attacks are not particularly sophisticated (Avertium, 2022).

Although aligned with those who seem to perceive Killnet as mere noise, Smith et al. (2022) admit that Killnet's activities within the context of the ongoing Ukrainian conflict reveal an intricate tapestry of strategic manoeuvring. The group's reactive cyberattacks are distinctly correlated with the evolving dynamics of the war and intricately linked with Moscow's broader geopolitical ambitions (also requiring its affiliates to ensure there will not be attacks on Russian targets). Paradoxically, Killnet’s leadership strives to dispel any notion of being a mere puppet entity manipulated by Russian state interests, highlighting their autonomy, while still pursuing recognition from Russian officials for their ‘contributions’ (Smith et al., 2022).

Smith et al.'s (2022) examination of the hacktivist group delineates how Killnet's actions are instrumental in cultivating a distinct cognitive environment and are significant to the extent that they focus on political mobilisation (as opposed to disruption or inflicting damage to the target). Regrettably, Smith seeks to distinguish this from any coercive action, sceptical of the "coercive utility of cyber operations". While the author of this dissertation agrees with Smith's portrayal of the strategic character of the activities of Killnet, the notion of coercion offered (or rather rejected) by Smith et al. remains excessively narrow. [10] By galvanising political mobilisation and imbuing cyberattacks with the potential to wield influence, Killnet's operations do assume a coercive dimension. The cyberattacks attempt to exert pressure on adversaries, threatening retaliation, (deterrence) and compelling a reconsideration of their stances vis-à-vis Russia.

Similarly to Killnet, NoName057, another group distinct from the former, specialises exclusively in executing DDoS attacks, targeting from utilities to transportation companies (Avast, 2022). While at the beginning of the year they focused mostly on Ukraine, by mid-June attacks appeared to expand to other targets and become more geopolitically motivated, with a noteworthy focus on the Baltic States. Their successful attacks are self-reported on a Telegram channel created in March 2022. Although they are not the only groups to disseminate this information online, a distinctive element of NoName057 is the central role given to the mediatic component since the group "heavily rel(ies) on volunteers' contributions to fuel and empower its offensive operations" (at least more than other groups like Killnet). According to B42 Labs (2023), NoName057 serves as a contemporary cyber militia supporting state propaganda and sponsored endeavours.

Another two groups causing ripples and standing out in the world of hacktivism are Xaknet and Legion. Xaknet appears particularly focused on targeting Ukraine instead of adopting a more international outlook. Beyond its DDoS operations, it should be remarked that, as revealed by researchers from Mandiant, there is a significant association between Xaknet and the Russian Main Intelligence Directorate Unit 26165, as well as the threat actor APT28 and CyberArmyofRussia_Reborn (Recorded Future, 2023). The US Cybersecurity & Infrastructure Security Agency released an advisory that further confirmed Xaknet's connection to Russia. According to this post, Xaknet issued a statement on March 2022 in which they proclaimed their commitment to working solely for the benefit of Russia (CISA, 2022).

The second group, Legion, identifies itself as a Cyber Spetsnaz or Cyber Special Forces unit and engages in operations that align with Killnet's objectives. It is believed to have emerged right before the war with Ukraine, around the end of January 2022, yet it was not until June that the motivations of the group became quite clear: in June, through the Telegram channel, Legion publicised its pursuit of an "elite cyber squad" under the name of "Sparta" whose main task would be sabotaging NATO nations, conducting cyber reconnaissance, leading to the destruction of Internet resources, "financial activity" and data theft (Recorded Future, 2023).

[10] According to Smith et al. (2022) argue that instead of coercion, Killnet's activites are "a mechanism for mobilising cadres and sustaining support for political and ideological goals internally, while simultaneously creating noise, hysteria, and hype over an artificially inflated threat among target and external audiences".

3.4 Discussion of the findings

In analysing the sample of cyberattacks, two key points become evident. Firstly, that there exists a great diversity in targets, types of attacks, hackers involved, and motivations. Secondly, bearing these factors in mind, companies and institutions (and their corresponding countries) can generally be considered to belong to one of two categories or groups – namely 1) Ukraine, and 2) the rest.

These two groups will be contrasted against a 'checklist' in order to establish whether these cyberattacks can actually be considered as instances of cyber economic warfare. The checklist below seeks to integrate ideas from existing literature into a single more comprehensive and inclusive conceptualisation of *cyber-economic warfare*, raising the threshold for what defines it and creating an operational framework for policymakers and relevant stakeholders to better identify it.

These criteria are as follows:

A. Are these isolated attacks or do they belong to a general trend or greater strategy?
B. Is there a (geo)political motivation behind the attacks? (From the perspective of the perpetrators, as well as the potential nation-state behind them.)
C. Are there any linkages between the perpetrators and nation-states? And if so, how close are these connections? Are hackers directed and financed by the state, do they act as proxies with indirect affiliations, or is their relationship characterised by tacit permission to conduct without prosecution their cyber activities?
D. Have these attacks targeted crucial economic targets? And have the attacks sought to economically impact the entities at hand (and their respective countries)? (Have they imposed strategic costs?)
E. Are these attacks instances of coercion? Or in other words, is the objective to coerce, deter, compel an enemy and/or is it sending a specific message?
F. Could these entities be understood as military targets, or do they exist as stand-alone targets|actions?
G. Are these disruptive, degradative or other types of attacks? What is the (potential) extent of the damage?

1. **Ukraine**

A.	**Greater strategy. Military?** Applied as part of Russia's grand strategy.
B.	**Yes.** The geopolitical motivation behind the attacks is clear, as the perpetrator is ultimately the Russian state. Thus, they are inherently geopolitical – being part of the greater context of the Russian justification for the invasion. These cyberattacks further serve as a tool to project power and assert dominance.
C.	**Yes.** These attacks have been carried out by APTs and have been traced back to different units of the GRU (and thus the Russian intelligence and security apparatus). Their relationship can be considered a *direct association,* as they are directed by the Russian state.
D.	**Yes.** Due to the highly important nature of the targets as well as the degradative type of attack (wiper malware). The targets include the national nuclear power

	company (state enterprise), an electricity supply company, the country's largest commercial energy operator, etc. However, it is difficult to infer to what extent these are economic targets, and what the economic impact was, as the specific entities targeted are often unnamed.
E.	**No.** Coercion, as a type of diplomatic strategy, is inapplicable due to the complete diplomatic breakdown between the two countries. There is nothing to pressure Ukraine towards on a political level (read: coerce), besides a military surrender. Thus, the attacks seek to undermine Ukraine's resistance more generally.
F.	**Military targets.** While also being economic targets. Due to the ongoing state of war, it is impossible to detangle these cyberattacks from other kinetic measures, and thus impossible to limit their scope to *only* the economic domain.
G.	**Degradative. Serious damage** (as it is bespoke wiper malware carried out by highly sophisticated groups). Some cyberespionage, albeit at a lower level.

2. The Rest

A.	**General trend. Potential General** (political) **Strategy.**
B.	**Yes*.** Depending on the actor. When the perpetrators are hacktivists, there is an explicit and clear political and ideological motivation. When the perpetrators are ransomware groups, only some have said to support Russia. Others have distanced themselves and call themselves apolitical (officially only being financially motivated), but have regardless never targeted states within the CIS (including Russia). This signals some level of tacit alignment. We further know of some instances of such groups communicating with the Russian state.
C.	**Yes*.** Varies depending on the actor and objective or type of cyberattack. See section B above. They have generally acted as proxies, with indirect relations (occurring on a voluntary basis). The minimum common denominator is that they enjoy the tacit permission of the Russian state to conduct their cyberactivities abroad without prosecution.
D.	**Yes*.** Cumulative economic impact. Impacts on a case-by-case individual level (including both direct and indirect costs) can only be inferred through extrapolation from external analyses. Since a great percentage of these attacks are ransomware, and due to the costly nature of such attacks, we can therefore deduce and assume substantial cumulative damages.
E.	**Yes.** Coercion and signaling. This depends on the type of attack. Depending on the target, Russia has different objectives. For example, it will want to compel EU countries to drop sanctions, halt their increases in defence spending, maintain energy dependence, etc.
F.	**Not military targets** - only economic targets. Despite the increased tensions, there is no ongoing war.
G.	**Disruptive attacks** (denial of service and ransomware) **and espionage.** Global damage is difficult to gauge on a granular case-by-case basis, but the damage is significant when considered holistically. Individually, on average, the damage is lower than in the case of the degradative attacks mentioned above.

In the case of Ukraine (group 1), the above given answers seem to more firmly correlate to the postulated definition/checklist for cyber economic warfare. Particularly regarding point G – economic damage, and C – links to the state. However, the aim does not appear to be to coerce and apply pressure towards a specific political outcome. The attacks are not an independent phenomenon, and can only be seen as following Russia’s overall military efforts.

The context is starkly different in the rest of Europe (group 2). Here, these attacks better correspond to the definition of cyber economic warfare, despite being harder to demonstrably link to Russia or to each other. This is owed to the fact that the cyber economic attacks would exist as an independent phenomenon (outside of a military context), with a large number of *yesses* (albeit with constant asterisks due to variations in actors’ modus operandi, nature of the targets and the attacks). By zooming out and seeing the bigger picture, the attacks cumulatively spell out a common trend – the weaponisation of cyberattacks for economic warfare.

4. CONCLUSION

This comprehensive analysis of the cyberattacks threatening the energy sector in the year 2022 serves as proof that cyber economic warfare is not merely a theoretical concept but a very real danger. Russia's actions during this period have demonstrated the potential havoc that can be wreaked upon nations through the strategic manipulation of their economies and how this can be achieved. The question now arises: could we see such cyber economic warfare again in the future? The answer, regrettably, is a resounding "yes." And it is imperative that we recognise that the impact of such attacks need not manifest in massive physical destruction.

As highlighted throughout this dissertation, there exist clear precedents for such actions, from cyber offensives operations to economic coercion, firmly rooted in Russia's strategic doctrine. Moscow possesses the means, with a pool of talented hackers and plausible deniability, and has compelling reasons to engage in these activities, standing much to gain from changes in the geopolitical landscape, and the possibility of exerting economic leverage over its adversaries due to longstanding interdependencies.

Moving forward, future studies must dig deeper into the effectiveness and utility of cyber economic warfare relative to other strategies or the use of economic and cyber warfare in isolation. Additionally, exploring the potential extension of such tactics to other critical economic sectors such as transportation and telecommunications could offer valuable insights. Lastly, while this dissertation has focused primarily on Russia, it is prudent to consider how other global powers, notably China, may employ similar tactics in the future. As the world becomes increasingly reliant on digital infrastructures and economic interdependencies, the study of cyber economic warfare becomes not just an academic exercise but a vital necessity for safeguarding international economic security and stability.

5. BIBLIOGRAPHY

Aljohani, Tawfiq. “Cyberattacks on Energy Infrastructures: Modern War Weapons” 2022, https://arxiv.org/ftp/arxiv/papers/2208/2208.14225.pdf

Allcot, Dawn. “Report: Cost of a Data Breach in Energy and Utilities.” *Security Intelligence,* Nov. 2021, https://securityintelligence.com/articles/cost-data-breach-energy-utilities/

Anghel, Suzana, et al. “The Future of EU Defence: A European Army?” *European Parliament,* Sep. 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652096/EPRS_STU(2020)652096_EN.pdf

Atwell, David, et al. “The Future of Cyber Conflict: The Coming Age of Cyber Persistence.” *PRISM*, vol. 9, no. 2, 2021, pp. 113-121, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-2/prism_9-2_113-121_Atwell-Portzer-McCurdy.pdf?ver=k11HUvaldhsIGIEaRbF5LA%3D%3D

Avast. “NoName057(16) Pro-Russian Hacker Group Targeting Sites in Ukraine and Supporting Countries with DDoS Attacks.” *Avast*. Sep. 2022. https://press.avast.com/noname05716-pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks

Avertium. "An In-Depth Look at Russian Threat Actor, Killnet." *Avertium Explore,* 2022, https://explore.avertium.com/resource/an-in-depth-look-at-russian-threat-actor-killnet.

B., Jamila, and Livia Tibirna. “The Energy sector 2022 cyber threat landscape.” *Sekoia*. Apr. 2023. https://blog.sekoia.io/the-energy-sector-2022-cyber-threat-landscape/

B42 Labs. “Data Insights from Russian Cyber Militants: NoName05716.” *Medium*. Apr. 2023. https://medium.com/@b42labs/data-insights-from-russian-cyber-militants-noname057-9f4db98f60e

Balteanu, Irina, and Francesca Viani. “The energy dependency of the EU and Spain” *Banco de España,* Jun. 2023. https://doi.org/10.53479/30253

Bateman, Jon, et al. “What the Russian Invasion Reveals About the Future of Cyber Warfare.” *Carnegie Endowment for International Peace*. Dec. 2022. https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667

Birol, Fatih. "Where things stand in the global energy crisis one year on." *International Energy Agency*. Feb, 2023, https://www.iea.org/commentaries/where-things-stand-in-the-global-energy-crisis-one-year-on.

Blank, Stephen, and Younkyoo Kim. "Economic Warfare a la Russe: The Energy Weapon and Russian National Security Strategy." *The Journal of East Asian Affairs*, vol. 30, no. 1, 2016, pp. 1-39,120-121. ProQuest, http://ezproxy.lib.gla.ac.uk/login?url=https://www.proquest.com/scholarly-journals/economic-warfare-la-russe-energy-weapon-russian/docview/1814169147/se-2.

Brenner, Susan. “Cybercrime, cyberterrorism and cyberwarfare” *Revue Internationale de Droit Pénal*, vol. 77, no. 3, 2006, pp. 453-466,

Burgess, Matt. “Leaked Ransomware Docs Show Conti Helping Putin from the Shadows.” *Wired*, Conde Nast, Mar. 2022, www.wired.com/story/conti-ransomware-russia/.

Busygina, Irina. “Russia– EU Relations and the Common Neighborhood.” *Taylor & Francis*, 2017. DOI: 10.4324/9781315443966

Caliskan, Murat, and Michel Liégeois. “The Concept of ‘Hybrid Warfare’ Undermines NATO’s Strategic Thinking: Insights from Interviews with NATO Officials.” *Small Wars & Insurgencies*, vol. 32, no. 2, 2021, pp. 295-319, DOI: 10.1080/09592318.2020.1860374

Caliskan, Murat. “Hybrid Warfare through the Lens of Strategic Theory.” *Defense & Security Analysis*, vol. 35, no. 1, 2019, pp. 40-58, DOI: 10.1080/14751798.2019.1565364

Canfil, Justin. “The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay.” *Journal of Cybersecurity*, Vol. 8, No. 1, 2022, https://doi.org/10.1093/cybsec/tyac007

Carter, Dylan. “Russian cyberwarfare targets both Ukraine and the West.” *The Brussels Times.* Jan. 2023. https://www.brusselstimes.com/358941/russian-cyberwarfare-targets-both-ukraine-and-western-europe

Chastand, Jean-Baptiste, et al. “Paris approves the building of Russian-led nuclear reactors in Hungary.” *Le Monde*, Apr. 2023, https://www.lemonde.fr/en/international/article/2023/04/28/in-hungary-paris-is-willing-to-help-build-russian-led-nuclear-reactor_6024637_4.html.

CISA. “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure” *CISA*. May. 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

CISA. “Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector.” *CISA*. Mar. 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a

Clarke, Aaron. "Hacking the Invasion: The Cyber Implications of Russia's Invasion of Ukraine." *Third Way,* Apr. 2022, www.thirdway.org/memo/hacking-the-invasion-the-cyber-implications-of-russias-invasion-of-ukraine.

Collins, Gabriel. “Russia’s Use of the ‘Energy Weapon’ in Europe.” *Baker Institute*, Jul. 2017, https://www.bakerinstitute.org/research/russias-use-energy-weapon-europe.

Cormac, Rory, and Richard J. Aldrich. “Grey is the new black: covert action and implausible deniability,” *International Affairs*. Vol. 94. No. 3. May 2018. Pp. 477-494. https://academic.oup.com/ia/article/94/3/477/4992414

Cornish, Paul. “The Vulnerabilities of Developed States to Economic Cyber Warfare.” *Chatham House*, June 2011, https://www.chathamhouse.org/sites/default/files/0611wp_cornish.pdf

Czyżak, Paweł. “Shocked into Action - EU Countries’ Energy Policies.” *Ember,* Jun. 2022, https://ember-climate.org/insights/research/eu-slashes-fossil-fuels/.

Datta, Pratim. “Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack”. *Journal of Information Technology Teaching Cases,* vol. 12, no. 2, Mar. 2021. pp.115–120. https://doi.org/10.1177/2043886921993126

Deamer, Lanna. "The DDoS threat for energy and utility companies." *Electronic Specifier*, Jan. 2018. https://www.electronicspecifier.com/products/cyber-security/the-ddos-threat-for-energy-and-utility-companies.

Delorme, Jacob, et al. “Cutting the Cord: Ending Europe’s Energy Dependency on Russia.” *Tony Blair Institute for Global Change,* Mar. 2022. https://www.institute.global/insights/geopolitics-and-security/cutting-cord-ending-europes-energy-dependency-russia.

Dupuy, Arnold et al. “Energy security in the era of hybrid warfare”. *NATO Review.* Jan 2021. https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html

ESET Research. "ESET Research: Russian APT groups, including Sandworm, continue their attacks against Ukraine with wipers and ransomware” *ESET Research*. Jan. 2023. https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-russian-apt-groups-including-sandworm-continue-their-attacks-against-ukraine-with-wipe/

European Commission Directorate-General for Energy. “High Volatility and Geopolitical Tensions Impact Electricity and Gas Market Developments in Q1 2022.” *European Commission,* Jul. 2022, https://commission.europa.eu/news/high-volatility-and-geopolitical-tensions-impact-electricity-and-gas-market-developments-q1-2022-2022-07-08_en.

Even, Schmuel. “Broad Economic Warfare in the Cyber Era.” *Cyber, Intelligence, and Security*, vol. 2, no. 2, Sept. 2018, pp. 85–109, https://www.inss.org.il/wp-content/uploads/2018/10/Even.pdf.

Faife, Corin. "Conti ransomware group discusses whether to target Russia in leaked chat logs." *The Verge*, 28 Feb. 2022, www.theverge.com/2022/2/28/22955246/conti-ransomware-russia-ukraine-chat-logs-leaked.

Ferris, Nick. “The hackers out for energy.” *The New Statesman*. May 2022. https://www.newstatesman.com/spotlight/sustainability/energy/2022/05/the-hackers-out-for-energy

Fix, Liana, and Caroline Kapp. “One Year After: How Putin Got Germany Wrong.” *Council on Foreign Relations,* Feb. 2023, https://www.cfr.org/in-brief/one-year-after-how-putin-got-germany-wrong.

Frąckiewicz, Marcin. “The Economics of DDoS Attacks and Mitigation Strategies.” *TS2.* Jun. 2023. https://ts2.space/en/the-economics-of-ddos-attacks-and-mitigation-strategies/

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security*, vol. 38, no. 2, 2013, pp. 41–73. JSTOR, http://www.jstor.org/stable/24480930. Accessed 5 Aug. 2023.

Glover, Claudia. “Has DarkSide returned? Notorious ransomware gang may be behind German oil attack.” *TechMonitor*. Feb. 2022. https://techmonitor.ai/technology/cybersecurity/german-oil-company-attack-blackcat

Gomez, Miguel Alberto. "Coercion and Cyberspace." ARI 102/2018, Real Instituto *Elcano,* 2018, https://media.realinstitutoelcano.org/wp-content/uploads/2018/09/ari102-2018-gomez-coercion-cyberspace.pdf.

Gompert, David C. and Hans Binnendijk, “The Power to Coerce: Countering Adversaries Without Going to War.” *Santa Monica*, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1000.html.

Greenberg, Andy. “Ukraine Suffered More Data-Wiping Malware Last Year Than Anywhere, Ever.” *WIRED*. Feb. 2023. https://www.wired.com/story/ukraine-russia-wiper-malware/

Greig, Jonathan. "Italy Warns of Cyberattacks on Energy Industry After Eni, GSE Incidents." *The Record by Recorded Future,* Sep. 2023, therecord.media/italy-warns-of-cyberattacks-on-energy-industry-after-eni-gse-incidents.

Greig, Jonathan. “BlackCat ransomware implicated in attack on German oil companies” *ZDNET*. Feb. 2022. https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/

Greig, Jonathan. "Russia-based hackers ramping up attacks on Eastern European energy sector.” *The Record.* Apr. 2023. https://therecord.media/russia-hackers-ramping-up-energy-sector-attacks

Grigas, Agnia. “Legacies, Coercion and Soft Power: Russian Influence in the Baltic States.” *Chatham House*, Aug. 2012, https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0812bp_grigas.pdf.

Gros, Daniel, and Farzaneh Shamsfakhr. “ENERGY PRICES AND INFLATION.” *CEPS.* https://www.ceps.eu/wp-content/uploads/2022/12/CEPS-Explainer-2022-09_Energy-prices-and-inflation.pdf

Hackenbroich, Jonathan, and Filip Medunic. “The Kremlin’s energy warfare.” *European Council on Foreign Relations*, Apr. 2022. https://ecfr.eu/article/the-kremlins-energy-warfare/

Hakala, Janne, and Jazlyn Melnychuk. “RUSSIA’S STRATEGY IN CYBERSPACE.” *NATO Strategic Communications Centre of Excellence.* 2021. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

Healey, Jason. "The Spectrum of National Responsibility for Cyberattacks." *The Brown Journal of World Affairs*, vol. 18, no. 1, 2011, pp. 57-70. JSTOR, http://www.jstor.org/stable/24590776. Accessed 19 Aug. 2023.

Herpig, Sven, et al. “Spotting the Bear: Credible Attribution and Russian Operations in Cyberspace.” *HACKS, LEAKS AND DISRUPTIONS: RUSSIAN CYBER STRATEGIES*, European Union Institute for Security Studies (EUISS), 2018, pp. 33–42. JSTOR, http://www.jstor.org/stable/resrep21140.7.

Hodgson, Quentin. “Understanding and Countering Cyber Coercion.” *CCDCOE.* 2018. https://www.ccdcoe.org/uploads/2018/10/Art-04-Understanding-and-Countering-Cyber-Coercion.pdf

“How the EU Has Been Supporting Ukraine.” *European Parliament News*, Jan. 2022, https://www.europarl.europa.eu/news/en/headlines/priorities/ukraine/20220127STO22047/how-the-eu-has-been-supporting-ukraine

Imperva. “What DDoS Attacks Really Cost Your Business.” *Imperva.* https://www.imperva.com/resources/resource-library/infographics/what-ddos-attacks-really-cost-your-business/

International Energy Agency. "Russia's War on Ukraine." *International Energy Agency*, https://www.iea.org/topics/russias-war-on-ukraine.

International Energy Agency. “Russia’s invasion of Ukraine has sparked a global energy crisis.” *International Energy Agency*. 2022. https://www.iea.org/reports/world-energy-outlook-2022/executive-summary

Iskandarov, Khayal, and Piotr Gawliczek. “Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point”. *Security & Defence Quarterly*. vol 40. no 4. 2022. pp.47-57. http://doi.org/10.35467/sdq/151038

James, Luke. "Energy sector: More cyber attacks in 2022 than ever before”. *Power & Beyond.* Mar 2023. https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a010c7a7e7d3/

Javier, Erick Nielson. "Economic Coercion: Implications to the Philippines and Possible Counters." *NDCP, National Defense College of the Philippines,* 2023, https://ndcp.edu.ph/economic-coercion-implication-to-the-philippines-and-possible-counters/.

Jones, Catherine. “Sanctions as Tools to Signal, Constrain, and Coerce.” *Asia Policy*, vol. 13, no. 3, 2018, pp. 20–27. JSTOR, https://www.jstor.org/stable/26497785.
Jun, Jenny. “THE POLITICAL ECONOMY OF RANSOMWARE.” *War on the Rocks*. Jun. 2021. https://warontherocks.com/2021/06/the-political-economy-of-ransomware/

Kalyanaraman, Sankaran. “Review of War by Other Means: Geoeconomics and Statecraft by Robert D. Blackwill and Jennifer M. Harris.” *Strategic Analysis*, vol. 41, no. 6, 2017, pp. 591-594, doi:10.1080/09700161.2017.1377897.

Kardaś, Szymon. “Conscious Uncoupling: Europeans' Russian Gas Challenge in 2023.” *European Council on Foreign Relations,* Feb. 2023, https://ecfr.eu/article/conscious-uncoupling-europeans-russian-gas-challenge-in-2023/.

Kaspersky. “Cyberwar in Ukraine leads to all-time-high levels of DDoS attacks.” *Kaspersky*. Apr. 2022. https://www.kaspersky.com/about/press-releases/2022_cyberwar-in-ukraine-leads-to-all-time-high-levels-of-ddos-attacks

Kennedy, Simon. “Cyberattack Economics.” *Bloomberg*. Mar. 2022. https://www.bloomberg.com/news/newsletters/2022-03-08/what-s-happening-in-the-world-economy-the-risks-of-cyberattacks

Kerner, Sean Michael. “Colonial Pipeline hack explained: Everything you need to know.” *techtarget*. Apr. 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Klimburg, Alexander, et al. “Why the energy sector's latest cyberattack in Europe matters.” *World Economic Forum*. Feb. 2022. https://www.weforum.org/agenda/2022/02/cyberattack-amsterdam-rotterdam-antwerp-energy-sector/

Krickovic, Andrej. “When Interdependence Produces Conflict: EU–Russia Energy Relations as a Security Dilemma.” *Contemporary Security Policy,* vol. 36, no. 1, 2015, pp. 3-26, DOI: 10.1080/13523260.2015.1012350

LaBelle, Michael Carnegie. “Energy as a weapon of war: Lessons from 50 years of energy interdependence.” *Global Policy*, vol.14, no. 3, Jun. 2023. pp. 531-547. https://doi.org/10.1111/1758-5899.13235

Lambert, Nicholas. “Brits-Krieg: The Strategy of Economic Warfare.” *Carnegie Endowment for International Peace*, 2017, carnegieendowment.org/sada/86922.

Lonergan, Erica, and Michael Poznansky. “ARE WE ASKING TOO MUCH OF CYBER?” *War on the Rocks*. May 2023. https://warontherocks.com/2023/05/are-we-asking-too-much-of-cyber/#:~:text=The upshot is that both,conventional tools that commonly fail

Lyngaas, Sean. “German intelligence agencies warn of Russian hacking threats to critical infrastructure.” *CyberScoop*, May 2020, https://cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/.

Maurer, Tim. Cyber Mercenaries: The State, Hackers, and Power. Cambridge University Press, 2018. DOI: https://doi.org/10.1017/9781316422724

McGraw, Gary. "Cyber War is Inevitable (Unless We Build Security In)" *Journal of Strategic Studies*. Vol. 36, No. 1, 2013. pp. 109-119. DOI: 10.1080/01402390.2012.742013

McLean, Elena V. "Economic Coercion." *The Oxford Handbook of International Political Economy*. May 2021. DOI: 10.1093/oxfordhb/9780198793519.013.2

Meister, Stefan. "A Paradigm Shift: EU-Russia Relations After the War in Ukraine." *Carnegie Europe*. Nov. 2022. https://carnegieeurope.eu/2022/11/29/paradigm-shift-eu-russia-relations-after-war-in-ukraine-pub-88476

Mendoza, Martha, and Dasha Litvinova. "Putin profits off US and European reliance on Russian nuclear fuel." *AP News*, Aug. 2023, https://apnews.com/article/russia-ukraine-war-us-europe-nuclear-exports-4129cbea2aaa69b1da5d09a41804f745.
NIST. "Cyber Attack". *NIST Glossary*. https://csrc.nist.gov/glossary/term/Cyber_Attack

Pascual, Manuel. "Why Russia has failed to win the cyberwar in Ukraine." *El Pais*. Feb. 2023. https://english.elpais.com/international/2023-02-14/why-russia-has-failed-to-win-the-cyberwar-in-ukraine.html

Rapnouil, Manuel Lafont. "Signal, constrain, and coerce: A more strategic use of sanctions." *European Council on Foreign Relations*. Jun. 2017. https://ecfr.eu/article/essay_signal_constrain_and_coerce_a_more_strategic_use_of_sanctions/

Ravich, Samantha. "Cyber-Enabled Economic Warfare: An Evolving Challenge." *Hudson Institute,* August 2015, http://prognoz.eurasian-defence.ru/sites/default/files/source/2015.08cyberenabledeconomicwarfareanevolvingchallenge.pdf.

Ravich, Samantha and Annie Fixler. "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare" *Center on Sanctions and Illicit Finance.* Feb. 2017. https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/22217_Cyber_Definitions.pdf

Recorded Future. "Dark Covenant: Connections Between the Russian State and Criminal Actors" *Recorded Future,* Sep. 2021, www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine.

Recorded Future. "Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine: Recorded Future." *Recorded Future*, Jan. 2023, www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine.

Reuters. "Timeline: The events leading up to Russia's invasion of Ukraine" *Reuters*, Mar. 2022. "https://www.reuters.com/world/europe/events-leading-up-russias-invasion-ukraine-2022-02-28/"

Ribeiro, Anna. "FROZENBARENTS Group Targets Energy Sector as Ukraine Remains Russia's Biggest Cyber Focus This Year." *Industrial Cyber,* Apr. 2023, https://industrialcyber.co/threat-landscape/frozenbarents-group-targets-energy-sector-as-ukraine-remains-russias-biggest-cyber-focus-this-year/.

Rohner, Natasha. “Russian Wrecking Crews Go Phishing with Worms and Wipers.” *Blackberry Blog*. Feb. 2023. https://blogs.blackberry.com/en/2023/02/russian-wrecking-crews-go-phishing-with-worms-and-wipers

“Russia and Germany Have De Facto Broken off Diplomatic Relations.” *Bne IntelliNews*, Apr. 2023, https://intellinews.com/russia-and-germany-have-de-facto-broken-off-diplomatic-relations-276679/

S&P Global Commodity Insights Team. “Energy Security Sentinel”. *S&P Global*. 2023. https://www.spglobal.com/commodityinsights/PlattsContent/_assets/_files/en/specialreports/oil/oil-security-sentinel.html

Sabin, Sam. “Colonial Pipeline ransomware attack's unexpected legacy.” *AXIOS*. May 2023. https://www.axios.com/2023/05/08/colonial-pipeline-ransomware-attacks-unexpected-legacy

Sgaravatti, Giovanni, et al. “National fiscal policy responses to the energy crisis.” *Bruegel.* Jun. 2023. https://www.bruegel.org/dataset/national-policies-shield-consumers-rising-energy-prices

Shagina, Maria. “Russia’s Demise as an Energy Superpower.” *IISS*. Aug. 2022. https://www.iiss.org/online-analysis/survival-online/2022/08/russias-demise-as-an-energy-superpower/

Shakeel, Irfan. "Cyberattacks Could Worsen the Global Energy Crisis." *AT&T Cybersecurity*, Dec. 2022, https://cybersecurity.att.com/blogs/security-essentials/cyberattacks-could-worsen-the-global-energy-crisis.

Slukhai, Sergii. "ECONOMIC WARS WITHIN THE RUSSIA-UKRAINE CONFRONTATION." *Ante Portas - Studia nad bezpieczeństwem,* Vol.2, No.11. 2018, DOI: 10.33674/2201817.

Smith, Maggie, et al. “What Impact, if Any, Does Killnet Have?” *Lawfare Media*. Oct. 2022. https://www.lawfaremedia.org/article/what-impact-if-any-does-killnet-have

Smith, Maggie, et al. “What Impact, if Any, Does Killnet Have?” *Lawfare Media*. Oct. 2022. https://www.lawfaremedia.org/article/what-impact-if-any-does-killnet-have

Smolanoff, Jason, and Megan Greene. “Cyber in 2023: Geopolitical and Economic Risks.” *Kroll*, Jan. 2023, www.kroll.com/en/insights/publications/cyber/2023-geopolitical-and-economic-risks-davos.

Soldatov, Andrei, and Irina Borogan. “Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities.” *CEPA*. Sept. 2022. https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/

Steiner, Hrafn. “Coercive Instruments in the Digital Age: The Cases of Cyber-Attacks Against Estonia and Iran.” *Swedish National Defence College, Department of Security, Strategy and Leadership*, 2014, https://www.diva-portal.org/smash/get/diva2:785614/FULLTEXT01.pdf

Steiner, Hrafn. “Cyber-Attacks as coercive instruments.” *Analys & Perspektiv,* no. 3, 2016, pp. 144–160, https://kkrva.se/hot/2016:3/steiner_cyber-attacks.pdf.

Stewart, Susan. “Consolidating Germany’s Russia Policy.” *Stiftung Wissenschaft und Politik*, Jun. 2023. doi:10.18449/2023C30

Sueur, Cypriaan, and Lisa Luijkx. “Lights Can Go out: Espionage & Disruption in the Energy Sector.” *Hunt & Hackett,* Feb. 2022, https://www.huntandhackett.com/blog/lights-can-go-out-espionage-and-disruption-in-the-energy-sector

Sussman, Bruce, and Christine Mok. “The Top 10 Countries Most Targeted by Cyberattacks.” *BlackBerry*. Sep. 2023. https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report

Thales's Cyber Threat Intelligence unit. “From Ukraine to the Whole of Europe: Cyber Conflict Reaches a Turning Point.” *Thales Group,* Mar. 2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point

Thornton, Rod, and Marina Miron. “Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow’s Strategic Thinking.” *The Cyber Defense Review*, vol. 7, no. 3, Summer 2022, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/09_Thorton_Miron_CDR_V7N3_Summer_2022.pdf?ver=0LhzDv4-cUkzkAqiTz401g%3D%3D

“Timeline: how the EU supported Ukraine in 2022” *European Parliament News*, Feb. 2023. https://www.europarl.europa.eu/news/en/headlines/world/20220519STO30402/timeline-how-the-eu-supported-ukraine-in-2022

Toulas, Bill. "Cyber espionage campaign targets renewable energy companies." *Bleeping Computer,* 23 Feb. 2023, https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/.

Trebesch, Cristoph, et al. “The Ukraine Support Tracker: Which countries help Ukraine and how?” *Kiel Institute for the World Economy*. Feb. 2023. https://www.ifw-kiel.de/fileadmin/Dateiverwaltung/IfW-Publications/-ifw/Kiel_Working_Paper/2022/KWP_2218_Which_countries_help_Ukraine_and_how_/KWP_2218_Trebesch_et_al_Ukraine_Support_Tracker.pdf

Troxell, John F. "Geoeconomics." *Military Review,* January-February 2018, www.armyupress.army.mil/Portals/7/military-review/Archives/English/Troxell-Geoeconomics.pdf.

Tully, Ryan, and Logan Weber. “Possible Futures for Russia’s CEEW Playbook.” *Foundation for Defense of Democracies,* Oct. 2022, https://www.fdd.org/analysis/2022/10/28/possible-futures-for-russias-ceew-playbook/

Tytler, James. "Hacking for the Kremlin: Russia, Ransomware and the West's Response." *Insights.* S-RM Infrom, 2023, https://insights.s-rminform.com/hacking-for-the-kremlin-russia-ransomware-and-the-wests-response.

Valeriano, Brandon, “ 'Cyber Coercion as a Combined Strategy', Cyber Strategy: The Evolving Character of Power and Coercion” *Oxford Academic*, May 2018, https://doi.org/10.1093/oso/9780190618094.003.0004.

Wadhwani, Sumeet. “Know Thy Enemy: Why RagnarLocker Remains a Significant Threat to Critical Infrastructure” *Spiceworks*. Sep. 2022. https://www.spiceworks.com/it-security/security-general/articles/ragnarlocker-ransomware-threat/

Wigell, Mikael, and Antto Vihma. “Geopolitics versus geoeconomics: the case of Russia's geostrategy and its effects on the EU” *International Affairs,* Vol. 92, no. 3. pp.605-627. May 2016. https://doi.org/10.1111/1468-2346.12600

Wigell et al. “Europe Facing Geoeconomics: Assessing Finland’s and the EU’s Risks and Options in the Technological Rivalry” *Publications of the Government’s Analysis, Assessment and Research Activities,* 2022:12. Feb. 2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163804/VNTEAS_2022_12.pdf?sequence=1

Wilde, Gavin. “Cyber Operations in Ukraine: Russia’s Unmet Expectations.” *Carnegie Endowment for International Peace*. Dec. 2022. https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607

Wolff, Guntram B. “The EU without Russian Oil and Gas.” *Bruegel*, Apr. 2022, https://www.bruegel.org/comment/eu-without-russian-oil-and-gas.

World Economic Forum. “Chapter 3: Digital Dependencies and Cyber Vulnerabilities.” *Global Risks Report 2022*, 11 Jan. 2022, https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities

Yanatma, Servet. “Europe’s ‘energy war’ in data: How have EU imports changed since Russia’s invasion of Ukraine?” *euronews.green.* Feb 2023. https://www.euronews.com/green/2023/02/24/europes-energy-war-in-data-how-have-eu-imports-changed-since-russias-invasion-of-ukraine

Zerter, Liam and Melissa Hudson. “The Impact of Cyberattacks on Stock Prices.” *Morningstar Sustainalytics*. Oct. 2022.

https://connect.sustainalytics.com/hubfs/INV/Thought Leadership/Sustainalytics_The Impact of Cyberattacks on Stock Prices_Sep 2022.pdf

Zilberman, Boris. “Don’t Underestimate Economic Side of Russia’s Cyber Warfare.” *The Cipher Brief,* 25 June 2018, www.thecipherbrief.com/column_article/dont-underestimate-economic-side-russias-cyber-warfare.

Zilberman, Boris. “Kaspersky and Beyond: Understanding Russia’s Approach to Cyber-Enabled Economic Warfare.” *Foundation for Defense of Democracies.* Jun. 2018. https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_RussiaCEEW.pdf