ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Cyberwarfare against Critical Infrastructures: Russia and Iran in the Gray Zone

Guillermo López-Rodríguez | Department of Political Science and Public Administration, University of Granada, Spain, ORCID: 0000–0001–8704–9007
Irais Moreno-López | Center of Political Studies, National Autonomous University, Mexico
José Carlos Hernández-Gutiérrez | Department of Political Science and Public Administration, University of Granada ORCID: 0000–0002–2855–1053

Abstract

The holistic nature of security in a hyper-connected world has increased the relevance of the cyber environment. One of the most relevant threats identified are the attacks against energy infrastructure. This article establishes a comparative study of cyber--attacks launched by Russia and Iran against energy-related infrastructure. Both countries are specialized in asymmetric strategies and tactics in which cyber has a core role. The research analyses both Iran and Russia´s main actions against energy supply infrastructure, studying the pursued objectives and identifying their potential political results. The document is structured as an initial theoretical approach to the use of asymmetric Gray Zone and hybrid strategies, focusing on the use of cyber-attacks by Rogue States. From this approach, the analysis reflects the political visions of Russia and Iran, linking it with Russia's actions in Ukraine, as well as the Iranian cyber offensives against western targets. The concluding section reflects on the effectiveness of these strategies with respect to the general strategy of both states.

Keywords

Iran, Russia, Cyberwarfare, Hybrid, Gray Zone

Received: 29.06.2023

Accepted: 16.10.2023

Published: 31.12.2023

Cite this article as:
G. López-Rodríguez, I. Moreno-López, J. C. Hernández-Gutiérrez "Cyberwarfare against Critical Infrastructures: Russia and Iran in the Gray Zone," ACIG, vol. 2, no. 1, 2023, doi: 10.60097/ACIG/162865.

Corresponding author:
Guillermo López-Rodríguez, Department of Political Science and Public Administration, University of Granada, Spain; ORCID: 0000–0001–8704–9007; E-MAIL: guillermolopez@ugr.es

1. Introduction

The geopolitics of energy in the 20th and 21st Centuries was controlled by the power of the Oil-States to be able to shut down the supply of oil and gas. The progressive energy transition has reduced the dependency on fossil fuels, and renewable energies have less scope to be used a tool of geopolitics as energy production becomes more decentralized. However, new threats are emerging, one of them being the supply interruptions due to cyber-attacks against critical infrastructure. One relevant example is the Russian attack against Ukraine in 2015 that left 250,000 people without energy supply [1].

Among the critical infrastructures the electricity network is one of the most relevant, due to the dependence of telecommunications, transport, the financial system or public security upon them [2]. Without electricity, the financial sector, emergency services and public institutions could be disrupted [3]. A disruption to the electrical network could also have fatal consequences: as an immediate result of the shutdown there could be dead and wounded, owing to fire, hypothermia, gas leaks, failures in the healthcare system or interruptions to the water supply [4]. The high level of interconnection between technological networks may pose a threat to state cybersecurity, as has been demonstrated in recent years with the cyber-attacks against national networks in certain countries [5].

Electricity networks are a priority target of the military and insurgents. For terrorist groups and organised insurgencies, it is cheap and easy to destroy high-voltage pylons or attack power stations. On the other hand, it is typical in military strategy is usual to plan kinetic offensives against power plants or analogous installations as part of bombing campaigns. Cyber-attacks are part of the portfolio of strategies of states [6]. It can be stated that the energy sector is exposed to a wide variety of attacks, with some of them falling within the framework of hybrid warfare [7]. In this sense, the United States has identified Russia, China, Iran and North Korea as critical threats to its energy sector [2].

This article analyses the cyber actions launched by Russia and Iran against the energy supply infrastructure of their adversaries. Both states are specialised in asymmetric strategies and tactics, defined by their lack of recognition, ambiguous objectives, and the use of proxy non-state actors. This is a comparative study that focuses on actions developed in order to achieve their geopolitical imperatives.

Due to this fact, the main objectives in this paper are to analyse the cyber actions as part of a broader strategy, with the further aim of

studying the most relevant cyber actions conducted against energy supply infrastructure. One of the most important contributions of the paper is to establish a link between the concept of the 'Gray Zone' and hybrid warfare, and applying this to the specific cases of Russia and Iran.

Starting from our approach to the use of asymmetric warfare by state actors, the analysis contains an outline of the geopolitical visions of Russia and Iran, so as to facilitate examination of their actions within the cyber domain. This research focuses on the Russian attacks against Ukraine and the Iranian cyber operations against Western targets. The conclusion reflects upon the effectiveness of these methods with reference to the general strategies of both states.

2. The Gray Zone and cyber strategies

Recent decades have shown the need for states to augment their military capabilities with more subtle ways of exerting their power [8]. For instance, power can be exercised incentives, bribery or coercion [9]. The liberal international trading environment provides opportunities for rapid economic development, while also providing illiberal states with ways of exploiting this environment in their favour to increase their relative power by evaluating their network sources [10]. While conventional warfare utilises a high number of communicative components, non-conventional actions are more difficult to capture and identify, combining economic, cultural or technological features in a geopolitical project [11].

In this respect, the use of energy as a geopolitical tool has become a key asset for shaping international relations [12]. This use might be driven by economic motives, political reasons, or even national security matters [13]. Using energy as a political and military resource has allowed states to influence other countries and their decisions by controlling energy supply or demand [14], as well as influencing control and access to their own resources or supply [15]. The availability of resources is considered a key element that determines the geopolitical behaviour of states [16], such that it can be turned into a target to be attacked conventionally and unconventionally by their adversaries.

Due to its relevance and the potential damage caused by its shortage, energy is instrumentalized in Gray Zone conflicts. The spectrum of competition space existing between states is positioned between

the polarities of absolute peace and conventional armed conflict [17]. The Gray Zone is a type of conflict in which actors seek limited political victories, acting within a murky environment which does not explicitly break the rules and values of the international world order [18]. The strategy implies a gradual conflict that seeks to modify components of the international system, using a combination of soft and hard power measures in non-conventional ways, making it difficult to prevent or respond to them [19]. This is a long-term approach, coordinating state and non-state actors and seeking to generate deterrence regarding the adversary [17].

The Gray Zone implies a temporary sustained confrontation that would not escalate to full-scale conventional war. The tools employed are economic and political pressure, energy blackmail or the use of cyberwarfare, both to reduce escalation of violence and to prevent retaliation [19]. This process is defined by a lack of clarity for the adversary, using ambiguity to weaken deterrence. However, both the revisionism of the international order and its alliances are a relevant component of the strategic objectives implied in this way of conflict [10]. The permissive and advantageous conditions are created by illiberal states such as China or Russia to effectively conduct operations in the Gray Zone against democratic countries. The lack of legal regulations allows authoritarian states to normalise new practices and tools in this Gray Zone. Authoritarianism is highly centralised yet bureaucratically flexible, which allows for more effective use of propaganda, legal national structures, economic pressure, and support for non-state proxies, in comparison to what democracies can employ.

The success of Gray Zone operations is based in the interconnection of political, informational, and economic domains [10]. In a more digitalised world, the cyber dimension has increased its relevance [17]. Cyber operations contribute to increasing the opacity of actions, due to the difficulties in assigning responsibility [20]. Due to this fact, cyberwarfare is closer to terrorism and guerrilla warfare than conventional warfare, being considered in some cases a force multiplier or a strategic tool in others [11]. The effects are even more pronounced, considering their low cost, disruptive potential and the high level of damage can be inflicted upon an adversary [20].

According to the literature, those states with aggressive geopolitical agendas are likely to enhance their virtual and automated tools in the future [21]. The cyber actions enable and require cooperation between public and private actors [17], which hinders the attribution of responsibility, while diversifying the objectives and increasing the

potential effects of network operations [22]. Cyberwarfare increases the attacker's advantages due to the element of surprise, which can hamper the opponent's ability to react when combined with other types of actions [11]. One of the key objectives can be critical non-military infrastructures, with unpredictable domino effects leading to scenarios that can lead to long-term blackouts with impacts on other services, such as healthcare or food supply [22].

3. The Russian and Iranian world view

Historically, Russia and Iran had maintained a strategic relationship towards a common enemy which they both conceptualize broadly as "the West"; this means, the United States and the European Union. The conceptual differentiation between Russia and The West has been a core element in the Russian cultural and philosophical tradition since the end of the 19th Century (Berlin, 1978). In the case of Iran, the 1979 Islamic Revolution formed the milestone for taking a religious, ideological and political distance from the West. The gulf expressed by both countries' leadership implies a different approach to the reality having its translation into politics [23]. This strategic agreement does not involve a dovetailing of ideological or moral perspectives between the leaderships of these two countries, but a common defensive view from their foreign policy standpoint and national interests that emphasizes the need to fight what they regard as western impositions, both in international, political and economic scenarios as well as in social life. There are two important elements that help to explain how the view of foreign policy in Iran and Russia is related to actions that lead to these kind of cyber-attacks on critical infrastructure, particularly on energy.

First, a traditional defensive view of Iran and Russia from what they call "the West" as a *de facto* international power headed formally and informally by the US and EU. This perception led to a specific view of their role in the international scenario, where "the West" is constantly trying to impose upon the rest of the world those views, lifestyle and policies that serve western interests. The transformation of international relations from a bipolar system into multipolarity implied that Russian elites would seek to be one of these poles [24]. Second, the view of both countries of foreign policy as a zero-sum game. Russia developed a particular combination of these two elements. Since Vladimir Putin's second term (2004–2008), Russia has re-emerged with the same policy stance as that adopted during the Cold War: once the menace from terrorism stopped as a common cause for United States and Russia, Vladimir Putin started

to distance himself from the West and began to claim the historical role of Russia – as heir of the USSR- in international politics. From that perspective, the very secure and already popular regime of the Russian president began to speak about a global shared leadership between the great powers, as existed from 1945–1991. The Russian invasion of Georgia in 2008 implied a rupture in the geopolitical relations between Western and Eastern countries. Prior to this military offensive, political analysts had assumed that the economic transformation in Russia would imply a closer approach to the West. In addition to the Georgian invasion, other key elements that widened the East-West gap were the Iranian nuclear program and the Afghan War [25].

The doctrine that nourished this perspective was called "Eurasianism", a long-forgotten term for this part of the world that no longer felt like part of Europe, and was not exclusively part of Asia either. This doctrine of Eurasianism forcefully vindicates the role of Russia as a great international power, that is, a kind of rationale for no western "intervention" in what they call the near abroad countries (meaning former USSR republics). The doctrine claims Russia's regional leadership of a symbolically constructed region called Eurasia in the name of power sharing across different regions of the world. According to Marcin Skladanowski [26], it was Dugin who founded "the Myth of Russian Exceptionalism", which is described as follows:

> *"The conviction of Russia's uniqueness, both in the past as well as the present" and this uniqueness has become the fuel to radicalize the anti-Western rhetoric of the Russian Federation because of its anti-Occidental identity awakening* [26].

In a similar way, from the moment the religious movement of Ayatollah Khomeini succeeded in Iran in 1979, a campaign of radical anti-westernization was undertaken by the new theocratic government. The country had earlier experienced a complicated decade because of the power struggle between a monarchy backed by the United Kingdom and the United States and headed by the Shah Mohammad Reza Pahlavi and several other political groups, such as communists and democrats led by Mohammad Mosaddeq, so in the 1960s Iran was a socially effervescent country with multiple perspectives on the future of Iran, which then vanished because of the banning and censorship arising from the Revolution.

A brief historical explanation is required in order to properly understand that in the 1970s the Soviet government and the newly established theocracy had nothing in common ideologically, while

both were committed to using anti-western rhetoric in order to sidestep the context of strong democratic inclinations and (after the Bandung Declaration) to legitimizing their own struggle against the impositions of capitalists from the west, announcing that they would be acting on their own terms concerning international relations. The sociocultural features of Iran have implied that, in spite of the regime's views, there is an active digital arena in the country, i.e., while the theocracy ruled according to the Ayatollah Khomeini's conservative views, they seem to have adapted very well to innovations in the Internet sphere. Since the expansion of the Internet, the digital arena has been used by politicians, civil society and journalists, as well as religious elites who had been using digital aspects for theological debates [27].

At the end of the first decade of the 21st Century it was clear that this common position shared by both Russia and Iran was not only maintained but reinforced by the constantly developing technologies, such as the Internet and its evolving resources. Evgeniy Morozov, a Belarusian dissident familiar with the multiple strategies of the Soviet and post-Soviet regimes, acknowledged that technology is not unconditionally on the side of democracy, and more than a decade ago he announced that the cyberutopian conception was about to detonate in the hands of its adherents. This refers to the idea that the Internet, by virtue of its mere existence and the socialization it engendered, would find a way to becoming the main tool for democratization and open societies, and therefore defeat authoritarian regimes [28]. Morozov himself explained how this idealistic perspective failed, such as during the so-called Iranian "Green Revolution" or the Green Movement of 2009[1].

The ideas of Morozov have become even more relevant now that we face the twin challenges of cyber-attacks and AI, and with Iran and Russia also having become skilful and frequent users of these resources for furthering their political and geopolitical objectives. Coincidentally, according to the timeline presented by United States Institute for Peace, both countries started launching cyber-attacks around 2008 and 2009 [29]. Globally, the Cybersecurity and Infrastructure Security Agencies (CISA) registered a 38% increase in cyber-attacks in 2022 [30]. Although not all cyber-attacks come from the state actors themselves, here we are going to refer only to cyber-attacks undertaken by the governments of Russia and Iran. Both countries had been accused of drastically increasing cyber-attacks from Israel and the US in 2022 and 2023 [30]. Cyberwarfare from these perspectives is highly effective for both countries: since it has specific targets and because of its mechanisms it might be able

1 —— Evgenii Morozov places the Green Movement or Green Revolution in Iran as one of the first collective and more illustrative movements greatly disappointed by the hopes of 'cyberutopianism'. Thousands of Iranians united in the streets of Tehran to speak out openly against the theocratic regime. Many of them organized the protest through Facebook, they even posted their precise location so others could join them in the street protests. The result, in terms of loosening the regime's tight grip, was a disaster. The political police traced the leaders of the Green Movement through geolocation, as many were subsequently arrested and harassed, including their families. In this case, the once supposedly liberating digital tools ended up aiding the persecution.

achieve its objectives with relatively low losses or no losses. Even so, this does not mean that this kind of attack is cheap to carry out.

4. Cyber-attacks on critical infrastructure: the strategy of Russia and Iran

The relevance of critical infrastructure for western countries' stability implies the analysis of cyber operations conducted by Russia and Iran. The low economic cost of the actions and the high impact in comparison with other kinetic attacks provides a justification for their use. In this section of the analysis, the research analysed the use of cyber operations in the framework of asymmetric actions, focusing on certain key operations. In the Russian case the analysis focused on the Ukrainian scenario, while Iranian operations demonstrate a higher diversity of targets and infrastructures affected.

4.1. Russia: hybrid warfare against Ukraine

The use of cyber strategies in Russia has been linked with informational warfare and influence operations. This is explained by the historical relevance of propaganda as a core element in political operations, a heritage from the Soviet times due to its long-term approach. Russia has extensively used trolls to manipulate, to create disinformation and to promote subversion. This use of cyber actions has been complementary to kinetic attacks against infrastructures which cause material damage, as happened in 2008 in Georgia and in 2014 in Ukraine [31]. The Russian invasion of Ukraine in 2022 has proved how hybrid warfare is a renewed, yet very aggressive way of attacking other countries' nervous systems, causing great damage at relatively little cost to the attacker. The very concept of hybrid war has been conceived of in terms of how Russia was able to find new vectors of attack – or what they call self-defence – since the annexation of Crimea in 2014:

> *The term Hybrid War or Warfare (HW) rose to prominence in defense and policy circles as well as in the media after the Russian annexation of Crimea in 2014. It was dragged out from the relative obscurity of military theory circles to become a mainstream term used to describe a myriad of seemingly different security and defense challenges to the West* [32].

Although the concept of Hybrid Warfare has been criticised it is still widely used, and it helps to explain several variations from the traditional conception of a physical war. The concept emerged first for

non-state actors who conducted operations with political or military objectives, then it also became part of the new military strategies for state actors. One of the main characteristics concerning Hybrid Warfare between states is the expansion of the battlefield:

> *In addition to blurred what is considered peace, conflict and war, hybrid warfare breaks the distinction between what is and what is not part of the battlefield... HW is both multimodal and employed on multiple levels at the same time, that comprises: the traditional levels of war – tactics, operation and field strategy- thereby accelerating the tempo at the strategic and tactical levels faster than a more conventional actor is able to do. Traditional physical spaces such as land, sea, air and space are increasingly accompanied by social and built spaces such as the political, economic, cultural and infrastructural and cyber* [32].

The concept of Hybrid Warfare refers not only to high-tech military capabilities and cyber weapons, but as Reichborn-Kiennerud and Cullen (2016) explain, the concept includes the cognitive and psychological factors also, which are key in achieving military objectives. Since the beginning of the Russian invasion of Ukraine in February 2022, there has been numerous significant cyber-attacks targeting Ukraine's energy sector. These attacks have had a significant impact on Ukraine's ability to generate and distribute electricity and have also caused widespread disruption to businesses and consumers. One of the most notable attacks was a distributed denial-of-service (DDoS) attack that targeted Ukraine's three largest electricity distribution companies in December 2021. The attack caused widespread outages, leaving millions of Ukrainians without power.

In February 2022, shortly after the start of the Russian invasion, Ukraine's national grid operator, Ukrenergo, was hit by a sophisticated cyber-attack that caused widespread power outages. The attack was attributed to Russia and was seen as a clear attempt to cripple Ukraine's infrastructure. In addition to the attacks on Ukraine's electricity grid, there have also been several attacks targeting Ukraine's oil and gas sector. In March 2022, a group of hackers calling themselves Killnet claimed responsibility for a cyber-attack that targeted Ukraine's state-owned oil and gas company, Naftogaz. The attack caused the company's website to go offline and disrupted its operations.

The cyber-attacks on Ukraine's energy sector have had a significant impact on the country's economy and have had a cumulative effect

when considering the consequences of the invasion. The attacks have caused billions of dollars in damage and have also led to a loss of confidence in Ukraine's energy sector. The attacks have also had a significant impact on the lives of ordinary Ukrainians, who have been forced to cope with power outages and other disruptions. The cyber-attacks on Ukraine's energy sector are part of a broader pattern of Russian aggression against Ukraine. The attacks are designed to weaken Ukraine's economy and infrastructure, and to make it more difficult for Ukraine to defend itself. The attacks are also a clear violation of international law and have been condemned by the United Nations and other international organisations.

The cyber-attacks on Ukraine's energy sector are a reminder of the growing threat of cyberwarfare. As the world becomes increasingly interconnected, cyber-attacks are becoming a common way for countries to wage war. The attacks on Ukraine are a wake-up call and highlight the need for countries to invest in cybersecurity and to develop strategies to deter and respond to cyber- attacks. However, western analysts say that many of the cyber-attacks inflicted by Russia against Ukraine have been quickly repaired, sometimes within hours, because of the highly skilled Ukrainian experts in these areas [33].

4.2. Iran: Cyber-attacks on critical infrastructure of western allies

Iranian cyber strategy is complementary to other influence operations in its areas of interest. Iranian geopolitics is based on generating deterrence by blocking the Hormuz strait or possessing ballistic missiles while deploying proxy actors on the ground, as happens in Syria, Lebanon, Yemen or Iraq. The strategy of using proxies has been employed in cyberspace also, which is a core feature of Iranian strategy [34]. Cyber capabilities have been extensively developed, thanks to the governmental cooperation with technological institutes and universities. In addition to scientific research, there are governmental investments in high-tech and communication companies. Most of these investments are direct from the Science Ministry, while others come from technological hubs [35].

Although we have already explained the key features underlying the tense relationship between Iran and the West over several decades, it is necessary to explain that Iran has conducted a long list of cyber-attacks since 2009, precisely when the radical anti-western president Mahmoud Ahmadinejad was elected. His aggressive rhetoric matched perfectly with the newly available tools at that time [28]. To

this purpose, Iran has developed both defensive capabilities against foreign aggression and against the regime's political rivals, as well as offensive capabilities to confront American superiority over digital infrastructures. The defensive capabilities are focused on protecting sensitive data and critical infrastructure against cyber-attacks. In the same manner, the Iranian government has developed measures against the coordination of anti-government groups, so as to prevent the introduction of western ideas in opposition to the regime. In contrast, offensive capabilities are developed as a complementary tool within an asymmetric strategy against their enemies [35].

Several analyses of tactics, techniques and procedures of Iranian cyberwarfare show similar patterns between the Iranian government and its proxies in the Middle East. This strategy has been widely employed since 1979, with Iran having a cohesive network in the region which also operates in the cyber domain. The network of actors is unstable and some of the organisations use similar resources, tactics and procedures. The similarities can imply confusion, with it being unclear as to who is behind the attacks or whether those responsible are acting under orders from the Iranian government, or whether proxies are acting independently with no direct instructions being given [36].

Iran's tense relationship with Israel has a long history, which starts in the religious and ideological terrain, but the conflict has escalated to political tensions and even overt threats in different periods since 1979. At the present time, the wide range of capabilities opened up by Hybrid Warfare has led Iran to commence an extensive sequence of operations within cyberspace to pursue objectives against countries perceived by the Iranian leadership as hostile. Iran has been – and still remains – a very active actor when it comes to cyber-attacks, and there are several groups that perform this kind of action. There have been a broad array of operations carried out since 2009, and one of the main strategies from Iran is to attack western allies in the Middle East, mainly Israel and Saudi Arabia [37][2].

One of the main attacks upon critical energy infrastructure was performed in 2012 against Saudi Aramco, "a company responsible for 10% of the world's oil supply at the time" [38]. This operation can be considered as industrial sabotage against the regional rival of Iran, which is a relevant ally of western countries [39]. The attack began on August 15, 2012, by means of malware called Shamoon, which began deleting and overwriting data in around 30,000 computers, and responsibility for this was claimed by a group called the Cutting Sword of Justice:

2 ——— For a complete timeline of Iranian cyber-attacks against different countries but mainly, United States, Israel and Saudi Araba see the USIP (May 3rd, 2023) report: Iran accelerates cyber-attacks. Available online https://iranprimer.usip.org/blog/2023/may/03/report-iran-accelerates-cyberattacks

> *The attacks were timed to coincide with Ramadan when most workers would be absent to allow the malware the maximum time to work unimpeded. The malware only infiltrated office computers and did not impact systems dealing with technical operations. Still, it grounded services to a halt, as office workers resorted to communications with typewriters and fax machines and gasoline refill trucks were turned away with no way to process payments. To mitigate the damage, Aramco purchased 50,000 hard drives, paying higher prices to cut the line and buy all the hard drives on the manufacturing line at several Southeast Asian factories* [38].

In the last decade, Iran has performed numerous cyber-attacks against several countries, mainly United States and its allies: continuous cyber-attacks against Israel, the United Kingdom, Australia and even Albania. An important feature of these actions is that they attack not only critical energy infrastructure but also infrastructure vital to health, as was the case in 2022 against Boston's Children's Hospital and on Israeli water facilities back in 2020 [37]. The theocratic government has also launched attacks during us elections.

> *The Office of the Director of National Intelligence said that it had "high confidence" that Supreme Leader Ayatollah Ali Khamenei authorized a cyber influence campaign during the 2020 presidential election. The online operation was intended to "undercut former President Trump's reelection prospects - though without directly promoting his rivals." Iranian cyber actors published more than 1,000 pieces of online content from several thousand fake social media accounts. Iran also sent threatening emails to Democratic voters, tried to exploit vulnerabilities on state election websites and attempted to hack the email accounts of political campaign officials* [37].

The attacks have continued during 2023 and will remain. In April 2023, Microsoft warned about the Iranian-linked group called Mint Sandstorm that has:

> *[...] started targeting critical U.S. infrastructure including energy companies, transit systems and seaports in 2021. The group gained access to sensitive systems "in support of retaliatory destructive cyberattacks [...] "The increased aggression of Iranian threat actors appeared to correlate with other moves by the Iranian regime under a new national security apparatus, suggesting such groups are less bounded in their operations."*

Regarding the complexity of the cyber-attacks from both countries, as a tool intended to destabilise or to act as a weapon (as done by Russia), it is expected that these attacks can and will be used widely in the future in many aspects, whether for criminal extortion, non-state actors and between States. International law has been left standing and it is highly unlikely that it could prevent this kind of action between states. The comparative case shows the relevance of the state as a core actor in cyberwarfare, which often sponsors non-state proxies as a means of avoiding attribution. In addition, it is relevant to consider the importance of public expenditure to improve cyber capabilities, as well as the coordination with scientific institutions and the private sector, which increase the complexity of the digital arena as a domain of the conflict.

4.3. The impact of cyber-attacks from Iran and Russia

The analysis and examples used to demonstrate that hybrid warfare is a widely used strategy for both Iran and Russia must also take into account the fact that its impact is somewhat ambiguous, just like the strategy itself. According to the literature review, a conventional conflict allows one to easily identify the main actors, their motivations and the consequences of their actions, while it is difficult to identify them in Gray Zone operations [11]. Our case study confirms that relations can be found between general strategies and specific actions, but due to the unconventional nature of the operations it is complicated to prove this entirely. As long as the perpetrators (groups of individuals) are possibly related to the regimes (both in Iran and Russia), they will probably remain as an important part of a clandestine or informal part of hybrid multimodal warfare.

In some cases, as happened in Georgia in 2008 or in Ukraine in 2014 [31], cyber operations were clearly used as a complementary tool for conventional Russian military actions. In those cases, cyberwarfare was a secondary means of supporting other types of operations having a defined authorship. Some of the Russian cyber operations could be included in the set of hybrid actions, as they had a connection with specific kinetic operations. Other actions, especially those related to energy infrastructure, would be more adequately classified within the Gray Zone spectrum, since they can condition further political negotiations [14]. In contrast, the Iranian operations in the cyber domain would be better classified as Gray Zone activities, as most of them were performed following political objectives to destabilise adversaries. Their actions would aim to generate deterrence in order to improve their geopolitical position [17]. According to this analysis, Iranian cyber operations involve a high number of

public and private actors [17], which increases the difficulty in clearly identifying the authors of the attacks.

As different modalities of hybrid or non-conventional operations can be easily tracked, as happens with proxy wars or some disinformation campaigns, cyberwarfare is even more obscure and difficult to analyse. Actors involved in cyber operations are multiple and not always directly linked with only one state, thus allowing for deflection of responsibility [20]. A further impact is that hybrid cyberwarfare has become a part of national geopolitical strategies and it will remain as such. It is important to acknowledge that while cyber-attacks are often initiated by Rogue States with authoritarian regimes, liberal western countries can indeed respond to these and fight back in the same ambiguous terms. When analysing cyberwarfare, there are immediate impacts from the actions involved, as happens with cyber-attacks against critical infrastructure, which are easy to identify. In contrast, it is even more difficult to fully prove the political long-term consequences of cyber operations conducted in the Gray Zone. Cyberwarfare as a tool for military operations produces clear effects in supporting kinetic actions, but those operations with geopolitical purposes are much more difficult to capture.

5. Conclusion

This research constitutes an initial approach to the use of cyberwarfare against targets belonging to the energy sector. In a hyperconnected globalized world, various kinds of critical infrastructure are vulnerable to cyber-attacks. The article is intended to present a comparative analysis of the use of cyberwarfare by Russia and Iran. These cases show how two rogue states have included cyber actions as an important tool within their general strategy based on asymmetric operations. As is evident from our analysis, the actions implemented at the operational level are perfectly coordinated, combining state and non-state actors and having a long-term approach of weakening their adversaries.

Their strategies include cyber actions in the framework of hybrid warfare. Despite this concept having been widely brought into question, it is still used in official speeches and analysis [32]. The cyber tools are inserted into the framework of Gray Zone conflicts, as their use can weaken the defences of adversaries. The consequences of cyber actions can imply cognitive and psychological victories which can increase the complexity of the adversaries' social environment. The case of Ukraine provides evidence for some of the direct effects

of cyber-attacks on energy infrastructure, such as blackouts and the interruption of normal business activities. Such actions have been mainly based on service denial, implying both material and reputational damage. The analysis has shown that since the beginning of the invasion of Ukraine, Russia has developed several cyber actions within the framework of a general strategy. The purpose of such actions has been to support conventional military operations, as well as to weaken an adversary's defence system and undermine the morale of its citizens.

In addition to Russia, Iran has conducted cyber-attacks over a long period of time. This fact shows the long-term approach of their strategy. In this research we have analysed various actions taken against oil infrastructure in Saudi Arabia, American healthcare facilities and water supply in Israel. In the Iranian case we can see a high diversity of targets across different countries, but at the same time they use cyberwarfare to complement other offensive and soft power strategies. The Iranian case is an interesting one to study, as the regime combines high-tech elements in the digital arena with an ideological structure established within the cognitive framework of the regime.

This article facilitates the exploration of future research avenues for conducting deeper examinations into operations carried out in the Gray Zone. As the cyber dimension is a core element in the strategies of certain states, we cannot ignore the relevance of social and human dimensions for understanding the full impact of cyberwarfare against adversaries. From an analytical perspective, it would be relevant to have greater knowledge of western cyber operations conducted against rogue states, in order to find parallels in their procedures. Other future lines of research could be focused on understanding the various effects related to deterrence aspects provided by cyber capabilities, as well as the various societal consequences arising from energy infrastructures being attacked. These lines of research could be strengthened by producing primary data through interviews with cyber experts to find weaknesses and strengths in the current energy systems. In the same way, it would be relevant to produce quantitative data regarding social perceptions about the consequences of a lack of energy supply on society, seeking to study social resilience in Western countries.

In addition, it is important to acknowledge the limitations of this paper. First, it is complex to analyse the phenomena of cyberwarfare, owing to its particular characteristics: the blurred attribution of responsibilities; the lack of internet regulation and law enforcement within cyberspace. Another important limitation is the feature of

non-state proxies linked to cyber-attacks to strengthen a state's political or economic objectives. It is equally difficult to measure the effectiveness of such attacks for achieving Iran and Russia's geopolitical goals. The analysis presented here clearly shows that the cyber-attacks are destabilising energy infrastructure, while legal loopholes and poor law enforcement, in conjunction with the ambiguous nature of the attacks themselves, makes the potential damage incurred difficult to acknowledge or confront.

References

[1] A. Pinedo Lapeña, "Ciberseguridad, geopolítica y energía," in *Energía y Geoestrategia*, Spanish Ministry of Defense, Madrid: Spanish Institute for Strategic Studies, 2022, pp. 159–196.

[2] K. Melligan, "The Vulnerability of the United States Electrical Power Grid," *Journal of Applied Business and Economics*, vol. 22, no. 7, pp. 155–163, 2020, doi: 10.33423/jabe.v22i7.3259.

[3] Z. Zhang, "Cybersecurity policy for the electricity sector: the first step to protecting our critical infrastructure from cyber threats," *Boston University Journal of Science & Technology Law*, vol. 19, no. 2, pp. 319–366, 2013.

[4] A. Yates, "Death modes from a loss of energy infraestructure continuity in a community setting," *Homeland Security & Emergency Management*, vol. 10, no. 2, pp. 587–608, 2013, doi: 10.1515/jhsem-2012–0048.

[5] E. Hatipoglu, S. Al Muhanna, B. Efird, "Renewables and the future of geopolitics: Revisiting main concepts of international relations from the lens of renewables," *Russian Journal of Economics*, vol. 6, no. 4, 2020, pp. 358–373, 2020, doi: 10.32609/j.ruje.6.55450.

[6] J.A. Lewis. (2010). *The Electrical Grid as a Target for Cyber Attack*. [Online]. Available: http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf [Accessed: Dec. 29, 2023].

[7] A. I. Ayerbe, *La ciberseguridad en el sector energético*, ARI 3/2020. Madrid: Real Instituto Elcano, 2020.

[8] J.S. Nye, "Soft power," *Foreign Policy*, vol. 80, pp. 153–171, 1990.

[9] J. S. Nye, *Soft power: The means to success in world politics*. New York: Public Affairs, 2004.

[10] D. Belo, "Conflict in absence of war: a comparative analysis of China and Russia engagement in gray zone conflicts," *Canadian Foreign Policy Journal*, vol. 26, no. 1, pp. 73–91, 2020, doi: 10.1080/11926422.2019.1644358.

[11] D. Ventre. *Cyberwar and Information Warfare*. London: ISTE, 2011.

[12] D. Yergin, "Ensuring Energy Security," *Foreign Affairs*, vol. 85, no. 2, pp. 69–82, 2006, doi: 10.2307/20031912.

[13] A. Sánchez-Ortega, *Poder y seguridad energética en las relaciones internacionales: la estrategia rusa de poder*. Granada: Editorial Universidad de Granada, 2012.

[14] S. Paltsev, "The complicated geopolitics of renewable energy," *Bulletin of the Atomic Scientists*, vol. 72, no. 6, pp. 390–395, 2016, doi: 10.1080/00963402.2016.1240476.

[15] G. Escribano, "Geopolítica de la energía: identificación de algunas variables," *Índice: Revista de Estadística y Sociedad*, vol. 46, pp. 12–14, 2011.

[16] J. Jordán, "Un modelo de análisis geopolítico para el estudio de las relaciones internacionales," Documento *Marco 04/2018, Instituto Español de Estudios Estratégicos*, 2018.

[17] J. J. Wirtz, "Life in the "Gray Zone": observations for contemporary strategists," *Defense & Security Analysis*, vol. 33, no. 2, pp. 106–114, 2017, doi: 10.1080/14751798.2017.1310702.

[18] J. W. Matisek, "Shades of Gray Deterrence: Issues of fighting in the Gray Zone," *Journal or Strategic Security*, vol. 10, no. 3, pp. 1–26, 2017.

[19] M. J. Mazarr, *Gray Zone: Understanding a Changing Era of Conflict*. Carlisle: United States Army War College Press, 2015.

[20] R. Stiennon, *Surviving cyberwar*. Plymouth: Government Institutes, 2010.

[21] E. Schmidt, J. Cohen, T*he new digital era: Reshaping the future of people, nations and business*. New York: Random House, 2013.

[22] A. Greenberg, *Sandworm: A new era of Cyberwar and the Hunt for the Kremlin's most dangerous hackers*. New York: Doubleday, 2018.

[23] B. Groys, "Russia and the West: The Quest for Russian National identity," *Studies in Soviet Thought*, vol. 43, no. 3, pp. 185–198, 1992.

[24] J. Mankoff, "Russia and the West: Taking the longer view," *The Washington Quarterly*, vol. 20, no. 2, pp. 123–135, 2007.

[25] E. Rummer, A. Stent, "Russia and the West," *Survival: Global Politics and Strategy*, vol. 51, no. 2, pp. 91–104, 2009, doi: 10.1080/00396330902860835.

[26] M. Skladanowski, "The Myth of Russian Exceptionalism: Russia as a Civilization and its Uniqueness in Aleksandr G. Dugin's Thought," *Politics, Religion and Ideology*, vol. 4, no. 20, pp. 423–446, 2019, doi: 10.1080/21567689.2019.1697870.

[27] N. Mina, *Blogs, cyber-literature and virtual culture in Iran*. George C. Marshall: European Center for Security Studies, 15, 2007.

[28] E. Morozov, The net delusion. *The Darkside of the Internet Freedom*. New York: Public Affairs, 2012.

[29] United States Institute for Peace. (May 03, 2023). *Report. Iran accelerates cyber-attacks*. [Online]. Available: https://iranprimer.usip.org/blog/2023/may/03/report-iran-accelerates-cyberattacks [Accessed: Dec. 29, 2023].

[30] Check Point Research. (Jan. 05, 2023). Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. [Online]. Available: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ [Accessed: Jan. 25, 2024].

[31] T. Maurer, G. Hinck, "Russia: Information Security meets cyber security," in *Confronting an axis of cyber? China, Iran, North Korea, Russia in Cyberspace*, F. Rugge, Ed. Milan: Institute for International Political Studies (ISPI), 2018, pp. 39–57.

[32] E. Reichborn-Kjennerud, P. Cullen. (2016). *What is hybrid warfare?* [Online]. Available: https://www.jstor.org/stable/pdf/resrep07978.pdf [Accessed: Dec. 29, 2023].

[33] The Economist. (Nov. 30, 2022). *Lessons from Russia's Cyberwar in Ukraine. Science and Technology*. [Online]. Available: https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine [Accessed: Dec. 29, 2023].

[34] L. Tabanski, "Iran's cybered warfare meets western cyber-insecurity," in *Confronting an axis of cyber? China, Iran, North Korea, Russia in Cyberspace*, F. Rugge, Ed. Milan: Institute for International Political Studies (ISPI), 2018, pp. 121–141.

[35] G. Siboni, S. Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs*, vol. 4, no. 3, pp. 77–99, 2012.

[36] J. G. Spataro, "Iranian cyber espionage". Master Thesis. Utica College, 2019.

[37] United States Institute for Peace. (May 3, 2023). *Report. Iran accelerates cyber--attacks*. [Online]. Available: https://iranprimer.usip.org/blog/2023/may/03/report-iran-accelerates-cyberattacks [Accessed: Dec. 29, 2023].

[38] United Against Iranian Nuclear. (2023). *Report: The Iranian Cyberthreat*. UAIN. [Online]. Available: https://www.unitedagainstnucleariran.com/history-of-iranian-cyber-attacks-and-incidents [Accessed: Dec. 29, 2023].

[39] S. Jones, S. (Apr. 26, 2016). *Cyber warfare: Iran opens a new front*. Financial Times.