Eksplorium *p*-ISSN 0854-1418
Volume 45 No. 1s, 2024: 27–50 *e*-ISSN 2503-426X

Thus, do they all: APTs as instruments of State-Sponsored cyber operations

[1]Luigi Martino, [2]Claudio Paya Santos, (Correspondence Author), [3]Juan José Delgado Morán

[1]Khalifa University Abu Dhabi, Bologna University, Italy

luigi.martino3@unibo.it.

https://orcid.org/0000-0002-7417-2898

[2]Valencia International University, Spain

claudio.paya@professor.universidadviu.com

https://orcid.org/0000-0002-1908-9960

[3]Pablo de Olavide University, Spain

jjdelmor@upo.es

https://orcid.org/0000-0002-9945-8235

Article Received: 20 September 2024, Revised: 25 October 2024, Accepted: 05 December 2024

Abstract: The use of cyberspace by state and non-state actors has transformed international politics in the contemporary age, blurring the lines between peace and conflict. This article delves into the subject of Advanced Persistent Threats and how often state actors deploy these sophisticated cyber tools to achieve their political, military, and economic objectives. Specifically, we examine the relationship between regime type and the propensity to engage in APT activities through a comprehensive review of recent literature and statistical analysis. Even if our findings reveal that authoritarian regimes are significantly more likely to deploy state-affiliated APTs than democracies, the significant result is that APTs are used both by democratic and authoritarian regimes to achieve their goals. The study also explores the dynamics behind APT attacks by multiple state actors, with their differences in intensity and frequency of operations. For this research, the chosen countries are China, the U.S., Russia, Iran, and North Korea. Furthermore, the study shows the collaboration networks between APT groups, particularly those targeting a common adversary. These implications highlight the need to address the evolving threats posed by state-sponsored APTs and ensure that global cyber defences can keep pace with the sophistication and scale of these attacks.

Keywords: Advanced Persistent Threats (APTs); Cyber Power; State-Sponsored Cyber Operations; Authoritarian Regimes and Cyber Attacks.

INTRODUCTION

The central premise of this study is that cyberspace, due to its significant socio-political implications, has to be recognised as one of the fundamental dimensions of power within international politics, a fact that is linked to the transformation of the state's role in the digital age and its impact on the global system (Choucri, 2012; Demchak, 2011). Indeed, in contemporary security policy, the proliferation of cyber technologies has wholly integrated with political, military, diplomatic, and economic resources. Through this convergence, states nowadays can further their interests by leveraging the full spectrum of their power. (Ben Israel and Tabansky, 2015; Dunn Cavelty, 2024).

To understand the global effects of the cyber sphere, it is helpful to conduct a cost-benefit analysis of the dimensions of warfare, where power is quintessentially displayed in international relations (Delgado et al, 2019). Starting with the sea domain, for example, building a warship requires a substantial budget, a privilege not all nations can afford; the same

situation applies to the space domain, where entry costs are even higher and demand complex organisational structures and high technological and economic capabilities. Similarly, the air domain features prohibitively high costs, as the costs of military aircraft and satellite systems can range from millions to billions of dollars. Conversely, the "cyber instrument" is characterised by significantly lower costs. For example, an internet connection can cost only a few dozen dollars per month, a high-performance computer a few thousand dollars, and sophisticated software can be developed by a single individual, a small team or even by AI (Payá et al, 2023) .

Moreover, the development of frameworks for understanding and evaluating how this instrument is then translated to "cyber power" reflects how academia recognises it for its role in shaping power dynamics, such as with the conceptualisation of power as both domination and empowerment (Dunn Cavelty, 2018; Haugaard, 2012), drawing on models such as Nye's Three Faces of Power (Nye, 2010) and the Betz and Stevens Four Dimension Model (Betz et al., 2011). Furthermore, the Integrated Capability Model (Klimburg & Tirmaa-Klaar, 2011) conceptualises cyber power as the outcome of distributed forces, highlighting the complexity of its origins and manifestations.

However, the pursuit of ranking "state power", as Baldwin (2016) noted, often leads to measurement challenges particularly pronounced in the context of cyber power indexes. This results in the empirical analysis of cyber phenomena facing criticism due to the complexities of data quality and the lack of standardised measurement (Shandler & Canetti, 2024). Utilising well-structured and peer-reviewed datasets, coupled with quantitative and qualitative approaches, can enhance the validity of cyber research. Indeed, as Shandler and Canetti suggest, a "tokenisation" of cyber operations, similar to the segmentation of globalisation studies, can facilitate the investigation of cyber-related phenomena through empirical observations and data. The result is an approach that acknowledges the multifaceted nature of cyber dynamics and promotes a more holistic understanding of multiple complexities. However, despite the aforementioned growing interdisciplinary interest in cyber operations, non-technical disciplines (such as social sciences-oriented studies) have paid limited attention to these aspects, and while technical fields have increasingly incorporated geopolitical considerations, social scientists have yet to fully explore the role of APTs as extensions of state power in the digital age.

Our study will attempt to cover this gap by showing the relation between the "APT instrument" and regime type by first starting from the state-of-the-art of cyber research, showing that even though the existing literature acknowledges the political dimensions of cyber operations, it often lacks empirical validation through concrete data and tends to rely on hypothetical scenarios rather than fact-based research. Following this, the study will examine the cases of APT Groups as they are employed by democratic and authoritarian regimes, focusing on the war in Ukraine as a case study of a complex digital battlefield. Finally, we will include an explanation and literature review of our methodologies for quantitatively examining the relation between the democracy index and the number of APT Groups for each examined country before reporting and discussing our findings.

Through this structure, our research can make three key contributions. Firstly, a comprehensive review of the recent literature on APTs used for cyber operations for political objectives and our quantitative research shows that statistically authoritarian countries are more likely to deploy state-affiliated Advanced Persistent Threats than democratic countries. Secondly, we include an empirical analysis of the involvement of APTs from the United States, China, Iran, North Korea, and Russia, specifically focused on the effects produced by their attacks. We also include a case study of APT attacks on the United States to draw possible partnerships between APTs against the same target category, acting as a disruption multiplier. Thirdly, we also suggest that the use of data in cyber-related research should be encouraged, to create data-driven frameworks that can, in due time, continuously enhance the quality and the interpretation of the findings. Moreover, we recommend greater attention to APTs and other cyber capabilities, ensuring these critical aspects are more thoroughly explored in research.

STATECRAFT IN CYBERSPACE: EVIDENCES FROM RUSSIA, CHINA, IRAN, NORTH KOREA AND U.S.

The evolution of cyberspace into a part of the battlefield has changed the dynamics of international relations, with state and non-state actors using it to push their objectives; yet, while anonymity and deniability attract a range of actors, the strategies and motivations that are behind their activities in cyberspace vary considerably and can be used to identify them. To proceed in this research, five nations were selected from among several key players in cyberspace to be analysed, specifically Russia, China, Iran, North Korea, and the United States. The reason why these five nations were picked is because they are indicated by the literature (Voo, Hemani, Cassidy, 2023) as among the top detaining the most cyber power for the year 2022, as well as having executed the most cyber-attacks since the year 2000, based on the European Repository of Cyber Incidents (EuRepoC, 2024) database, merged with the APT Groups and Operations (cyb3rops, 2024). From Russia's measured aggressions and China's quest for information dominance to the targeted economic espionage of Iran and North Korea, each of these states utilises cyberspace in a manner reflective of its broader national security goals. Notably, even democracies such as the United States can engage in offensive cyber operations, which blurs the line between offence and defence in the digital domain even more (Kellog, 2018).

Proceeding to defining each actor, since the Russian cyberattacks on Estonia in 2007, cyberspace has emerged as a strategic arena where various state and non-state actors engage in confrontations. Even though their behaviours differ considerably, not only in their objectives and strategies but also in their methods and underlying motivations, they all exploit cyberspace’s advantages (Demchack, 2011; Martino, 2023). Beginning with Russia itself, Moscow has demonstrated its cyber capabilities through destructive cyberattacks, with operations such as NotPetya, with Lin (2022) and Levite (2023) arguing that Russia restrained its top-tier cyber assets to avoid escalation and retaliation from Western countries, possibly reserving them for future NATO confrontations. This is also motivated by cyber capabilities being often single-use, as the vulnerabilities they exploited are usually fixed in the aftermath.

Following with China, its cyber strategy is rooted in its strive for information dominance across multiple domains (Jinghua, 2019). According to Dean Cheng, Chinese cyber

operations encompass extensive information-gathering activities, for which they integrate electronic warfare, network warfare, and psychological operations to collect data. The Cyber Units of the People's Liberation Army prioritise the seamless collection, management, and exploitation of information, to support offensive and defensive operations (Beltran & Liz, 2019). A strategy that involves not only military targets, but also economic and political ones, and reflects China's concept of comprehensive national power (Jinghua, 2019; Cheng, 2017).

Moving on, both Iran and North Korea access cyberspace for intelligence-gathering operations, aimed at supporting policy decisions and engaging in industrial espionage and economic theft to boost their military and civilian sectors. At the same time, however, they each exhibit unique characteristics. Iran, notably, employs its cyber capabilities for punitive missions against perceived "traitors" (Couretas, 2024). Whereas North Korea's cyber operations, driven by an ongoing need for economic resources, heavily rely on the activities of the Lazarus Group APT and its subgroups (Recorded Future, 2023).

Finally, while most data on cyber-attacks focuses on non-democratic countries, we recognise that democracies also engage in offensive cyber activities, such as the United States. The U.S. are recognised as the leading "superpower" at a technological and cyber level (Gilli & Gilli 2019), with the strategy of "persistent engagement" or "defend forward" serving as a cornerstone of the U.S. behaviour in cyberspace, through which they target both cybercriminals and adversarial APTs. For instance, in April 2021, the Department of Justice executed a court-authorised operation to copy and remove malicious web shells from hundreds of vulnerable U.S. computers running on-premises versions of Microsoft Exchange Server software. This operation responded to attacks by HAFNIUM, a threat group believed to be affiliated with the Chinese government (Brumfield, 2022). Moreover, federal spending on cyber activities has significantly increased, with $2.6 billion allocated to contractors in 2017: a 65% rise from 2016 (Mahnoy, 2021). These contractors are tasked with environment preparation and cyber tools development, both of which require penetration of adversarial computer networks. Environment preparation also involves infiltrating enemy cyberspace to assess capabilities, intentions, and potential threats (Mahnoy, 2021).

As for the offence, the United States has demonstrated a cautious and measured approach in deploying offensive cyber operations, even against non-state actors such as the Islamic State (ISIS). In 2016, when the U.S. decided to use cyber-sabotage operations against ISIS, it did so only after considerable deliberation, and the operation was conducted with a clear structure, coordinated through an inter-agency task force, with Cyber Command taking a leading role (Mahnoy, 2021). A second example of this more "cautious" approach is that the U.S. typically deploys cyber-attacks at a later stage of a conflict, as opposed to the beginning. These facts can suggest a more substantial commitment to respecting the law while also focusing on minimising collateral damage; however, these late responses represent a limitation, as cyber-attacks in retaliation tend to be as efficient as they are rapid.

This paragraph demonstrated that state behaviour in cyberspace varies widely, with different strategies representing national security priorities and methods. States such as Russia, China, Iran, and North Korea pursue aggressive—albeit anonymous—activities tailored to their unique goals, whether it be information dominance, economic theft, or punitive missions.

Meanwhile, democracies like the United States have embraced the potential of offensive cyber operations, showcasing how the lines between defence and offence can blur in this domain.

APTS AS SOURCE OF STATE POWER PROJECTION?

The strategic and organised nature of APTs involving or linked to state actors has been a focal point of cybersecurity research. The term "advanced persistent threat" is defined as:

> Characterised by greater sophistication and skill, rapid collaboration, and increasingly structured relationships to overwhelm complex network security mechanisms—oftentimes from the inside. Their motivation is becoming increasingly profit-focused, and their modus operandi includes persistence and stealth. It includes possible state-sponsored actors whose effects contribute to long-term influence and exploitation campaigns, as well as devastating effects to facilitate military action. Their signatures include the use of zero-day exploits, distributed agent networks, advanced social engineering techniques such as spear phishing, and long-term data mining and exfiltration. Their flexibility and robust kitbag of tools and techniques makes the advanced threats particularly difficult to defeat with today's technology-heavy network security focus. (Schmidt et al. 2008, 3)

The literature around cyber operations, particularly on APTs, centres on the distinctions between conventional cyber-attacks and these more sophisticated and constant threats. In particular, one of the main differences is that APTs are often financed with substantial resources and advanced expertise provided by nation-state actors, which allows them to carry out prolonged and technologically advanced attacks (Challa, 2022). Interestingly, Olszewski (2018) suggests that APTs represent a novel form of military activity by states in cyberspace. As such, it can be inferred that with the militarisation of APTs, we have reached a significant evolution in the states' use of cyberspace, where these groups become extensions of the state power with an already documented reach. Specifically, Wilusz et al. (2022) report that multiple countries have already identified APTs within their border, showing how widespread these threats are. Moreover, their research shows how nation-states tend to use APTs to exploit software vulnerabilities to secure advantages in the military, political, or economic spheres; a fact that indicates that the deployment of APTs to pursue their national objectives is a critical issue within international security studies. The ethical and operational challenges posed by APTs are also a significant concern within the academic community.

Moreover, Guerrero-Saade (2015) discusses how the association of APTs with nation-state attacks raises questions about states' willingness to engage in cyber espionage and destructive cyber activities, raising ethical dilemmas regarding state conduct in cyberspace and the implications this could have for international stability. For example, Huang (2022), in examining Chinese APT operations within the APEC region, suggests that the Beijing views APTs as a crucial tool of national power, that compels other states in the area to adopt countermeasures to mitigate their impact.

Another aspect that is explored in the literature, is the how much governments are involved in the sponsorship of APTs and, as such, responsible for their proliferation. Indeed, Kose (2021) highlights that APTs are typically state-sponsored hacking groups, engaged in cyber espionage and other illicit activities, which goes to show the significant influence of state

actors in the cyber domain, further complicating international efforts to regulate cyber operations.

As a result of this type of issue, Charney (2014) addresses the legal implications of such state-sponsored APTs, advocating for the establishment of international norms to govern state behaviour in cyberspace and arguing that the misuse of the "APT instrument" by states not only endangers the direct victims, but also poses a broader risk to global cybersecurity. Further expanding on the ethics of cyber operations, Guerrero-Saade (2018) states that many APT groups are either integrated into or closely aligned with state apparatuses, an integration that complicates efforts to attribute cyberattacks and holds states accountable for their actions in cyberspace. Buzatu (2022) also adds that the increasing destabilisation of peace and security in cyberspace can be primarily attributed to state-sponsored APT groups, which infiltrate and control both state and commercial computer systems.

This goes to show that APTs are indeed instruments of power and are used by states in cyberspace to further their aim. As such, a growing threat and phenomenon such as this one should be met with enhanced research and cooperation, to address these challenges in an evolving cyberspace, where the line between peace and conflict continues to be further blurred.

APTS, AUTHORITARIAN AND DEMOCRATIC ACTORS AND LESSONS LEARNED FROM THE WAR IN UKRAINE

Advanced Persistent Threat Groups (or APTGs) from authoritarian countries such as Russia, China, Iran, and North Korea and democratic countries like the US, France, Israel, or the Five Eyes alliance all exhibit significant differences in their objectives, methodologies, and impacts. In this respect, Lemay et al. (2018) provide a systematic survey of publicly available reports on APT actors, indicating not only that state-sponsored APTs are a well-accepted phenomenon in cybersecurity, but providing also a substantial differentiation between APTs sponsored by authoritarian or democratic regimes (Luque et al, 2023).

Indeed, according to the survey, as well as Katagiri (2024) and Hunter et al. (2022), authoritarian regimes often deploy state-sponsored APTs in order to perform espionage, sabotage, or exercise political influence, frequently targeting critical infrastructure, government entities, or key industries to gather intelligence, disrupt operations, and exert geopolitical power (Payá et al, 2015; 2023). For example, China's APTs have been involved in extensive intellectual property theft and economic espionage, while Russia's operations, such as those attributed to APT28 (Fancy Bear), have focused on political interference and destabilisation efforts. North Korea and Iran have been linked to financially motivated cyberattacks aimed at evading international sanctions or conducting their assertive foreign policies.

Differently, according to the empirical evidence provided by Lemay et al. (2018), democratic nations primarily focus their APT efforts on defensive measures, cyber-threat intelligence sharing, and countering malign cyber activities (Rodríguez et al., 2023). While they also engage in cyber espionage, their operations are often more restrained by legal and ethical considerations, while also protecting democratic institutions. The Five Eyes Alliance would exemplify this cooperative approach, with member countries sharing intelligence to

enhance collective cybersecurity resilience. Despite the relevance of the content provided by Lemay et al., this kind of analysis fails to highlight a precise relationship between the use of APTs and international conflict, concluding that democracies are prone to utilising APTs solely for defensive purposes (Liz, 2024; 2023). In particular, the main issue in such classification lies in the non-linear relationships between cyber operations and the political systems at the international level. For instance, this perspective does not account for cases like the "Olympic Games operation" conducted by the United States and Israel against Iran via the Stuxnet worm, which, as Al-Rabiaah (2018) suggests, can be considered a precursor to an APT. Therefore, the Stuxnet case exemplifies the inherent complexity in attributing only a specific type of operation - offensive or defensive - to only one kind of regime. Thus, positions like those of Lemay et al. tend to oversimplify the problem, whereas the relationships between the use of APTs (or other state-sponsored cyber operations) and political regimes tend to be more complex. Indeed, further examples of APTGs sponsored by democratic regimes are the Animal Farm APT, attributed to French developers, the Regin platform linked to the Five Eyes intelligence alliance, and the Equation Group, associated with the United States. These APTGs are characterised by very refined capabilities, such as the possibility of deploying complex malware such as EvilBunny and Babar, modular espionage platforms, and firmware infection techniques. The use of such tools from Democratic states can potentially undermine the principles that these democracies claim to uphold, by blurring the line between offensive and defensive cyber operations.

This issue's complexity is also evident in contexts such as the Russo-Ukrainian war: here, both sides engage in offensive cyber operations, with over one hundred different cyber actors being involved, according to the CyberPeace Institute (2023), including using APTs, in order to achieve their political and military objectives, regardless of the nature of the regime from which these operations are launched.

For example, on the eve of the invasion, Russia launched a cyberattack on Viasat's European satellite network, disrupting internet services for many Ukrainian customers and causing communication breakdowns in government and business sectors (Willett, 2022). The attack was executed using AcidRain, a wiper malware deployed by Sandworm, a group associated with the Russian Military Intelligence (GRU) (Vijayan, 2024), which was also responsible for another notable instance of an attack that was integrated between cyber and military forces, directed at Ukraine's power grid, which caused a blackout preceding a missile attack in late 2022 (Maschmeyer, 2024). This represented an evolution in Russia's cyber-kinetic integration, which suggests improved capabilities from past experiences, which should prompt researchers to evaluate the effectiveness of these integrated attacks, as case studies like Bateman's analysis of the Dnipro operations show limited operational benefits despite tactical successes (Healey, 2024).

Offensive cyber operations can also erode trust in weapons systems or physical infrastructure. For example, in late 2022, a Russian-affiliated hacker claimed to have gained illicit access to Delta, a Ukrainian battle-management system, posting screenshots of sensitive military locations. Such operations, even if not detected, can cause a loss of trust, as subtle

malicious manipulation of command-and-control telemetry or disturbances in targeting latency could wreak havoc across an operational theatre.

In addition to these cases, cyber capabilities were and are used mainly to collect information. As seen in the war in Ukraine, Russia did not use (intentionally or not) the same destructive magnitude attack as NotPetya, while using similar malware but without the aim to spill over to other targets (or even states) (Maschmeyer, 2024). Regarding this, it appears as such that scholars tend to agree that Russian cyber capabilities are primarily focused on gathering intelligence to destroy targets, rather than using cyber-attacks to achieve results on their own (Baetman, 2022; Beecroft, 2022; Levite, 2023; Lin, 2022).

At the same time, Ukraine's defence posture in 2022 was different from 2014 due to the active collaboration and assistance from NATO, the European Union and private companies such as Microsoft and Google, among many others, to actively build a cyber shield for Ukraine cyber infrastructure (Martino, 2023). Nevertheless, Russia has shown to hold advanced capabilities in cyber arsenal, as shown by attacks such as NotPetya. These efforts have required Ukraine to retaliate, notably through the IT Army of Ukraine, formed under the guidance of Mykhailo Fedorov, the Minister of Digital Transformation. The IT Army has engaged in offensive cyber operations against Russia, by leveraging a decentralised approach where the it coordinates attacks through Telegram channels with its agents, democratising participation in offensive actions. Their targets have included prominent Russian entities such as Lukoil, Gazprom, and various banks, that were especially subjected to distributed denial-of-service (DDoS) attacks. While Ukraine might not possess the same level of sophisticated cyber weaponry as some nation-states, their innovative methods for mobilising a "cyber army" have proven effective in disrupting Russian operations. Beyond the IT Army, groups affiliated with the Security Service of Ukraine (SBU), the country's primary intelligence agency, have also been implicated in targeted cyberattacks against Russian infrastructure and government websites.

METHODOLOGY

Given that the main limits of research conducted so far are represented by lack on the assessment of the "political side" of cyber operations, we have decided to focus our analysis on extracting the APTs involved in offensive cyberattacks, which, as stated by Katagiri (2024), represent a significant component of the cyber threat landscape due to their sophisticated nature and the often-prolonged duration of their operations. By searching for already known group presented in EuRepoC, merged with APT Groups and Operations Database it was possible to assess their activities and involvement in political oriented aims. This type of classification allows further analysis on APTs as proxies of states and to follow the patterns of their strategy on launching cyber operations.

Given that the research hypotheses are oriented to validate or refuse the evidence that non-democratic countries are more prone to use APT that democratic regimes, the Democracy Index 2023 (The Economist Intelligence Unit, 2024), compiled by The Economist, will be used to evaluate the regime type of each state actor included in our analytical cluster. This will allow for a differentiation between the roles of democracies and autocracies in cyber operations and

the types of cyberattacks. To ensure consistency with our dataset, we created an innovative and ad hoc Cyber Weighted Democracy Index calculated using the following formula:

$$\text{Weighted Democracy Index} = \frac{\sum_{i=1}^{n}(D_i \times C_i)}{\sum_{i=1}^{n} C_i}$$

Where:

$$D_i = \text{Democracy score for year } i$$

$$C_i = \text{Number of cyberattacks in year } i$$

$$n = \text{Total number of years with recorded cyberattacks}$$

The weighted index provides a more accurate reflection of the political context during periods of heightened cyber activity.

Similarly, Doucouliagos and Uluba¸so˘glu (2008) used weighted average partial correlations in their meta-analysis of democracy and economic growth, ensuring that more reliable studies had a more significant influence on the overall conclusions. While Iwin´ska et al. (2019) employed stratification by government effectiveness, income levels, and corruption to explore the nuanced relationship between democracy and environmental quality, effectively weighting their analysis to account for varying impacts of these factors. Even in our research topic, this kind of research strategy based on stratification method serves as a form of weighting by highlighting the importance of different contextual variables.

By adopting a similar approach in our *Cyber Weighted Democracy Index,* we can provide a temporally sensitive analysis that reflects the dynamic nature of cyber threats and the political context in which they occur[i]. Given the cybersecurity landscape and the escalating international political tensions, exemplified by the Russo-Ukrainian war and the recent Middle East conflicts following the events of October 7th, it is imperative to have up-to-date analyses on the regime types of countries[i].

While Polity V's most recent data is from 2018, The Economist's Democracy Index provides insights up to 2023, and offers a more relevant perspective to understand the political environment that influences cyber threats[ii].

This methodology is also justified by the fact that the use of APTs by state actors – particularly non-democratic ones – raises important questions about the relationship between regime types and the propensity to engage in advanced cyber operations, as well as the broader implications for international security and cyber governance (Babb, 2022; Hunter et al., 2022; Katagiri, 2024). This is because, as discussed previously, the long-term cyber capabilities constituted by APTs are among the most sophisticated cyber weapons that countries could employ to achieve a strategic objective in cyberspace, and are often associated with states due to the significant resources and strategic planning required for their deployment and maintenance. It is their "persistent" nature that allows for continuous intelligence-gathering operations, repeated intellectual property thefts, or even the manipulation of critical infrastructures, and that makes them very powerful tools in achieving national objectives (Sanz et al., 2024).

FINDINGS AND DISCUSSION: APTS & WEBS OF POWER

As established by the qualitative research, the deployment of APTs by states has emerged as a pivotal aspect of modern cybersecurity and international relations. Whether authoritarian regimes are more likely than democratic states to deploy state-affiliated APTs is a question of how political systems, methods and objectives influence cyber strategies. The statistical analysis that we provide in this research indicates that there is compelling evidence to support this notion, and reveals the significant differences in how authoritarian and democratic regimes engage in cyber operations.

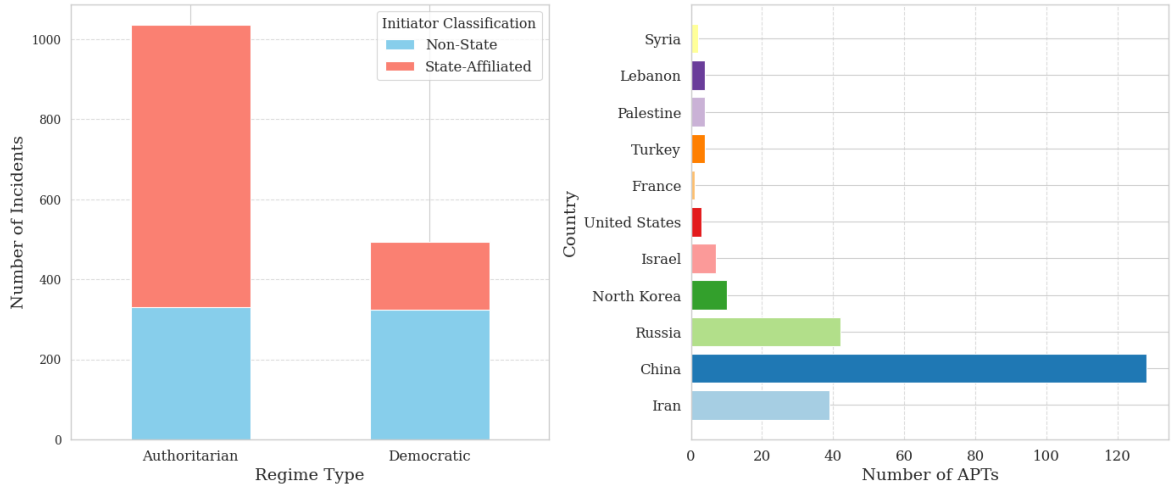


Figure 1. Relationship between Regime Type, APTs and Country affiliation

Chi-square tests reveal a disparity between authoritarian and democratic regimes in the use of state-affiliated APTs. Authoritarian states in particular have been linked to 705 instances of state-affiliated cyber threats, compared to just 170 in democratic countries. While the deployment of non-state threats remains relatively balanced (287 for authoritarian and 273 for democratic states), the *p-value* of 5.18e-35 highlights the profound association between regime type and the likelihood of using state-sponsored cyber operations. This data suggests that authoritarian regimes are not only more inclined but possibly even better equipped to deploy such sophisticated tools, unconstrained by the legal and ethical principles that often limit their democratic counterparts, as indicated by the literature. The disposition of authoritarian states to leverage cyber capabilities - and APTs - as an extension of state power could reflect their political methods and systems, where control, surveillance, and coercion are critical to maintaining stability and projecting their power in the world. Indeed, with insights from APT cyberattacks retrieved from EuRepoC are validated by the APT Groups and Operations Database, it can be that non-democratic countries have overall employed more unique APTs than the democratic ones. While the majority of nations, including democratic and non-democratic states, have a relatively low number of APTs, there are a few examples that do stand out. Figure 1 shows that specific non-democratic countries, such as Russia and China, have a significantly higher number of APTs compared to other nations, suggesting that they may focus on developing and deploying additional and more powerful cyber capabilities, to conduct espionage or, potentially, as a means of asserting their geopolitical influence.

Moreover, the intensity and frequency of APT attacks also illustrate how much and to what degree different states utilise these instruments. Figure 2, which maps cyberattack intensity versus frequency, reveals that groups like North Korea's Lazarus Group and Russia's Sofacy have conducted numerous cyberattacks with varying intensity levels. Differently, APT groups from democratic countries, such as the United States' Equation Group, tend to engage in fewer but more intense operations. This difference suggests that assertive foreign policies, such as those of authoritarian states like China and Russia, are connected with a higher number of cyber activities. In contrast, the opposite is true for democratic countries. The data also indicates a positive correlation between the sophistication of APTs and their success rates, a fact that goes to show states' significant investment of resources when they view cyber capabilities as integral to their national security apparatus, such as with APTGs (Martino, 2024).

Indeed, APTs are often considered the paragon of offensive cyber capabilities, reserved for the most impactful operations capable to deliver high-impact and frequently surprising blows to adversaries, a fact that makes them particularly valuable in the context of interstate conflict. As observed by DeVore and Lee (2017), the single-use nature of APTs - coupled with their capacity for significant, and sometimes lasting impact - means that states often hold these tools in reserve, to use during wartime or other types of crises. This approach is supported by the patterns observed in authoritarian states, where the deployment of APTs is mainly linked to periods of international tension or conflict.

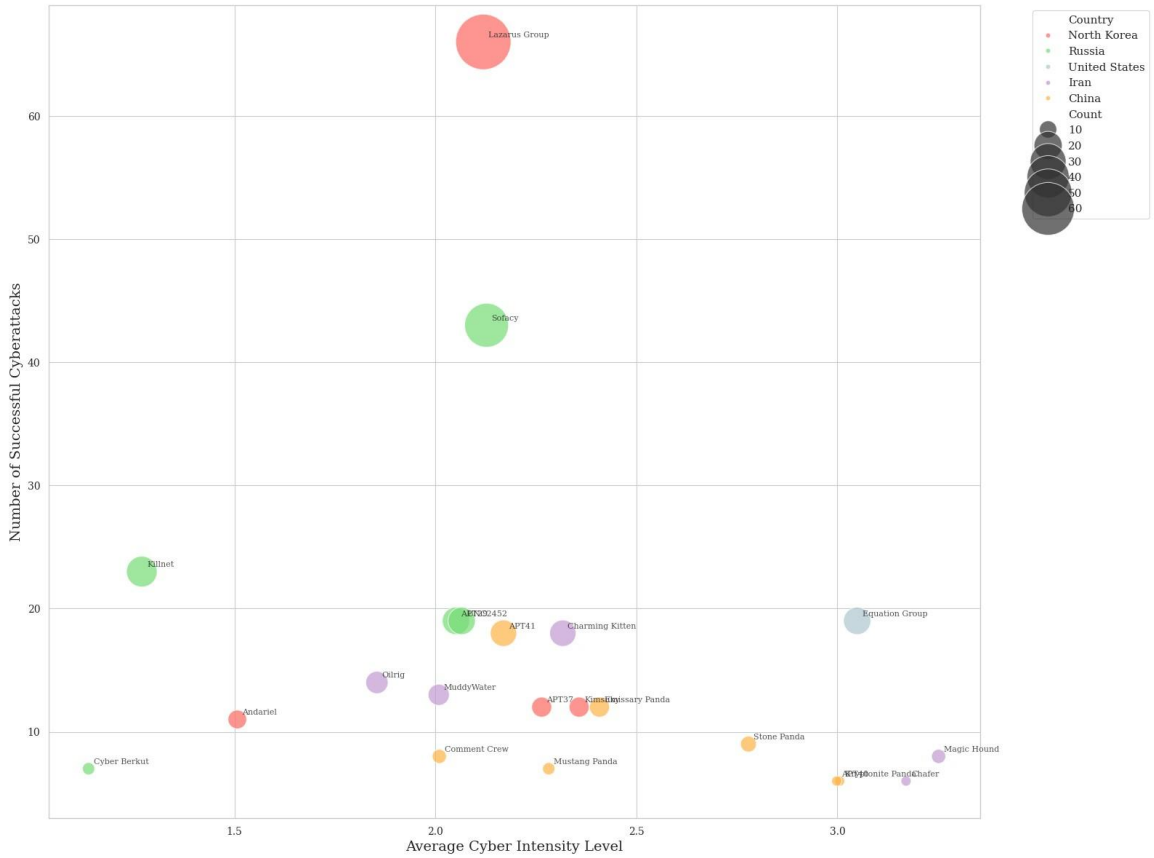


Figure 2. APT Cyberattacks: Intensity vs Frequency by Country

Furthermore, one of the most essential starting points for the future of research in APTs lies as such in understanding the possibility of collaboration between different APTGs, as well as between these and other entities in cyber space, particularly those with a common adversary. The preliminary analysis presented in this study examines the network of APTs targeting the United States over a 50-day period, highlighting instances where multiple groups attacked the same target category (e.g., military or government) within the same timeframe. The resulting network, as depicted in Figure 3, shows a central hub with the APT groups of APT1, Cozy Bear, PLA Unit 61398, and the Lazarus Group as a "collaboration group". These APTGs are not only prolific attackers but also key players in the world of cyber threats, capable of exerting significant damage, and it is interesting how they appear to be targeting one objective in a specific period of time.

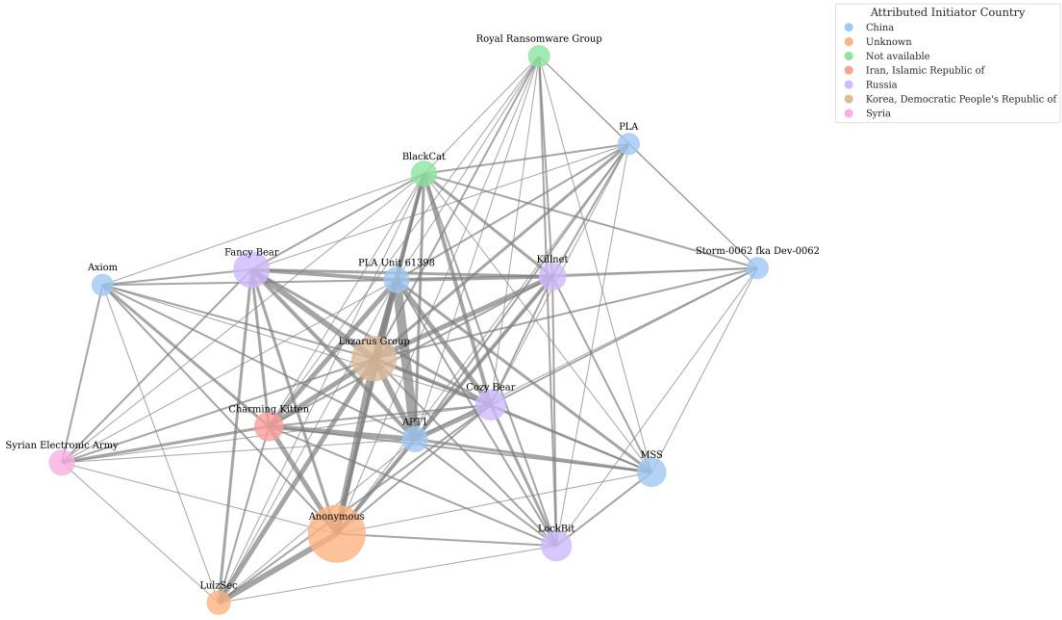


Figure 3. APT Collaboration Network over fifty days (Attacks on the United States)

Moreover, Figure 3 also shows the growing relationship between APTGs and cybercrime organisations, a phenomenon that makes the landscape of cyber threats even more complex, with groups such as BlackCat, offering Ransomware-as-a-Service on Russian-language forums while also increasingly adopting APTGs' techniques. This "cross-pollination" between APT groups and cybercriminals improves each other's capabilities, leading to more effective and damaging operations. Indeed, research shows that APTs have consistently utilised tools from the dark web, such as Remote Access Trojans (RATs) and exploit kits, developed initially for criminal purposes but now integral to state-sponsored cyber espionage and data exfiltration efforts (Krebs, 2024). While the opposite is also true, as cyber criminals are adopting APT-like strategies, such as shifting their focus from individual end-users to organisational networks, and employing advanced methods such as spear phishing and deep network infiltration (Aharoni, 2021). This interdependence between state-sponsored and non-sponsored group suggests the possibility of coordination and shared objectives which complicates the efforts to defend against these threats.

Finally, another layer of link between different groups is represented by political alliances, which often extend into cyberspace, with groups like the Syrian Electronic Army (SEA) allegedly operating under Iranian direction. The SEA's connections to groups like Charming Kitten and Hezbollah also show how state-backed cyber operations can leverage non-state actors to extend their reach and influence (Sanger & Schmitt, 2015).

The analysis of state-affiliated APTs highlights the need for a multidisciplinary approach to cybersecurity research, one that integrates political science with technical cybersecurity expertise. The number of patterns shown in this research, as well as the evolution of cyber threats, show that as the cyber instrument evolves so must our understanding of the motivations, strategies, and collaborations that drive these operations. As such, future research should make use of novel machine learning techniques to analyse the Tactics, Techniques, and Procedures employed by APTs, along with the digital infrastructure of their victims, with the objective of spotting patterns as well as connection between different nodes, such as the ones reported in this research between groups of cyber criminals and APTGs. Such studies would enhance our ability to predict and defend against cyber threats, and would ultimately contribute to more effective and proactive cybersecurity strategies (Martino, 2024).

CONCLUSION

Cyberspace, cyber-attacks and APTs have not fundamentally changed the balance of power in international politics. However, they have undoubtedly evolved the tools and methods at the statecraft's disposal. As a result of the low entry barriers and the potential to project power covertly, the capabilities of states and non-state actors to project influence have been enhanced. States such as the United States, China, Russia, Iran, and North Korea have integrated cyber capabilities into their strategic arsenals, with cyber power providing these states with a new avenue to achieve their strategic objectives.

What this study has shown, is that the methods employed between these actors differ substantially. While the Advanced Persistent Threat instrument is evidently used by all examined actors, authoritarian regimes are significantly more likely to deploy state-affiliated APTs compared to democratic countries. These findings have also shown their strategic use by authoritarian states to achieve long-term national objectives through continuous intelligence gathering, intellectual property theft, and critical infrastructure manipulation; the approach that is employed in this instances is a "resource-centric" approach, for which authoritarian countries, while capable of deploying highly calibrated and sophisticated attacks (such as with NotPetya or the VIASAT attacks), often prefer to retain them for future use, in instances where these can favour the ongoing struggle on the kinetic battlefield. These findings emphasise the political nature of cyber-attacks, which are more and more aligned with geopolitical interests and have become instruments of power in international politics.

Finally, even even if the democracies are prone to utilising APTs solely for defensive purposes, this implies that APTs are in any case part of their political-military "portfolio" in cyberspace. Indeed, if we were to assume that only authoritarian regimes engage in offensive APTs and democratic regimes engaging in defensive APTs, we would be stunned when put in front of the Stuxnet case. This oversimplification in the problem of classification (or

attribution) of the relationships between the use of APTs (or other state-sponsored cyber operations) and political regimes shows a much more complex reality, such as is evident in contexts such as the Russo-Ukrainian war, where both sides engage in offensive and defensive cyber operations, including using APTs.

Consequently, what this research has shown, is that proper quantitative and qualitative research on empirically assessing the "political side" of cyberspace can allow to avoid oversimplifying (or even naïve) assumptions, helping understand the multifaceted nature of cyber conflicts and the diverse motivations behind state-sponsored cyber activities.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors

FUNDING ACKNOWLEDGEMENT

This work was partially supported by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

DATA AVAILABILITY STATEMENT

The replication script and all datasets used in this research are available at https://doi.org/10.7910/DVN/0PIMZB.

Appendix A. Figure Details

A.1. Figure 2: APT Collaboration Network over a 50-day period (Attacks on the United States)

This figure visualises the collaboration network of Advanced Persistent Threat (APT) groups involved in cyberattacks on the United States. The network graph was constructed by analysing APT groups that conducted attacks in the same 50-day period and on the same category target. Edges represent the frequency of joint attacks. Node sizes reflect the number of attacks attributed to each APT group, and colours indicate the country attributed.

Appendix B. Statistical Summary Tables

B.1. Democratic and Non-Democratic Countries

Table B1. Cyber Weighted Democracy Index by Country

Initiator Country	Num Attacks	Weighted Score	Weighted Democracy Index	Regime Type	Democracy Status
Afghanistan	2	4.96	2.480000	Authoritarian (2-2.99)	Non-Democratic
Albania	1	6.41	6.410000	Flawed Democracy (6-6.99)	Democratic
Algeria	3	10.89	3.630000	Authoritarian (3-3.99)	Non-Democratic
Argentina	1	6.84	6.840000	Flawed Democracy (6-6.99)	Democratic
Armenia	10	40.09	4.009000	Hybrid Regime (4-4.99)	Non-Democratic
...					
United States	58	468.05	8.069828	Full Democracy (8-8.99)	Democratic
Uzbekistan	1	1.95	1.950000	Authoritarian (1-1.99)	Non-Democratic
Venezuela	3	11.05	3.683333	Authoritarian (3-3.99)	Non-Democratic
Vietnam	11	34.47	3.133636	Authoritarian (3-3.99)	Non-Democratic
Yemen	4	8.96	2.240000	Authoritarian (2-2.99)	Non-Democratic

To compute a binary classification of "Democratic" and "Non-Democratic," we use the threshold that separates "Flawed Democracies" from "Hybrid Regimes." The appropriate threshold is a score of 6.00. This is because "Flawed Democracies" have scores of 6.00 and above, whereas "Hybrid Regimes" and lower categories have scores below 6.00. The full list of the Cyber Weighted Democracy Index is available at: https://doi.org/10.7910/DVN/0PIMZB

REFERENCE LIST

[1] Aharoni, I. (2021). *The Ongoing Reciprocal Relationship Between APTs and Cybercriminals*. [online] SecurityWeek. Available at: https://www.securityweek.com/ongoing-reciprocal-relationship-between-apts-and-cybercriminals/.

[2] Al-Rabiaah, S. (2018). *The 'Stuxnet' Virus of 2010 As an Example of A 'APT' and Its 'Recent' Variances*. [online] IEEE Xplore. Doi:https://doi.org/10.1109/NCG.2018.8593143.

[3] Anne-Marie Buzatu (2022). Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace. *Cyber Peace*, [online] pp.236–242. Available at: https://www.academia.edu/85347897/Advanced_Persistent_Threat_Groups_Increasingly_Destabilize_Peace_and_Security_in_Cyberspace. https://doi.org/10.1017/9781108954341.015

[4] Antulio J Echevarria, II (2021). *War's logic: strategic thought and the American way of war*. Cambridge, United Kingdom; New York, NY: Cambridge University Press. https://doi.org/10.1017/9781316135730

[5] Austin, G., Tay, K.L. and Sharma, M. (2022). *Great-Power Offensive Cyber Campaigns: Experiments in Strategy*. [online] IISS. Available at: https://www.iiss.org/research-paper/2022/02/great-power-offensive-cyber-campaigns/

[6] Babb, C.E. (2022). *Digital Dictators: How Different Types of Authoritarian Regimes Use Cyber Attacks to Legitimize Their Rule*. [online] Available at: https://repository.library.carleton.ca/downloads/js956g84q.

[7] Baetman, J. (2022). *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*. [online] Available at: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

[8] Baldwin, D.A. (2016). *Power and International Relations: a Conceptual Approach.* Princeton University Press. https://doi.org/10.23943/princeton/9780691170381.001.0001

[9] Beecroft, N. (2022). *Evaluating the International Support to Ukrainian Cyber Defense*. [online] Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

[10] Betz, D.J. and Stevens, T. (2011). *Cyberspace and the State: Towards a Strategy for Cyber-Power*. London: Taylor and Francis.

[11] Bossetta, M. (2018). The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy. *Journal of International Affairs*, [online] 71(1.5), pp.97–106. Available at: https://portal.research.lu.se/en/publications/the-weaponization-of-social-media-spear-phishing-and-cyberattacks.

[12] Brumfield, C. (2022). *U.S. government offensive cybersecurity actions tied to defensive demands*. [online] CSO Online. Available at: https://www.csoonline.com/article/573597/u-s-government-offensive-cybersecurity-actions-tied-to-defensive-demands.html.

[13] Buchanan, B. (2017). *The Cybersecurity Dilemma*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001

[14] Buchanan, B. (2020). A National Security Research Agenda for Cy. *Center for Security and Emerging Technology,*. [online] doi:https://doi.org/10.51593/2020CA001.

[15] Challa, N. (2022). Unveiling the Shadows: A Comprehensive Exploration of Advanced Persistent Threats (APTs) and Silent Intrusions in Cybersecurity. *Journal of artificial intelligence & cloud computing*, pp.1–5. doi:https://doi.org/10.47363/jaicc/2022(1)190.

[16] Charney, S. (2014). *Governments and APTs: The Need for Norms*. [online] Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtU.

[17] Cheng, D. (2017). *Cyber dragon: inside China's information warfare and cyber operations*. Santa Barbara, California: Praeger, an imprint of ABC-CLIO, LLC. https://doi.org/10.5040/9798400636431

[18] Cheng-Hua , H. (2022). *Chinese APTs and the Political Influences in the APEC area*. [online] Available at: https://is.muni.cz/th/ovujl/Chinese_APTs_and_the_Political_Influences_in_the_APEC_area_.pdf.

[19] Council on Foreign Relations (2024). *Connect the Dots on State-Sponsored Cyber Incidents - Operation Aurora*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/operation-aurora#:~:text=Operation%20Aurora%20was%20a%20series.

[20] Couretas, J.M. (2024). *Cyber Operations*. John Wiley & Sons. https://doi.org/10.1002/9781119712121.ch1

[21] Cruz Beltrán, J.L & Liz Rivas, L. (2019). El perfil del ciberterrorista: la utilización de medios informáticos con fines terroristas, en; "El conflicto y su situación actual: del terrorismo a la amenaza híbrida", coord. por Carlos Espaliú Berdud, CIVITAS, pp. 159-173. https://doi.org/10.5281/zenodo.14562806

[22] Cyb3rops (2024). *APT Groups and Operations*. [online] apt.threattracking.com. Available at: https://apt.threattracking.com.

[23] CyberPeace Institute (2021). *Cyber Dimension of the Armed Conflict in Ukraine*. [online] CyberPeace Institute. Available at: https://cyberpeaceinstitute.org/%20publications%20/cyber-%20dimensions-%20of-%20the-%20armed-%20conflict-%20in%20-%20ukraine-%20q4-2022/.

[24] Damien Van Puyvelde and Brantly, A.F. (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Polity.

[25] Delgado Moran, J. J.; Mazurier, P.A. & Paya Santos, C. A. (2019). The race to securitize the arctic in a post-cold War scenario. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 4(1), 59-64. http://hdl.handle.net/10272/17180

[26] Demchak, C.C. (2011). *Wars of disruption and resilience: cybered conflict, power, and national security*. Athens; London: University Of Georgia Press. https://doi.org/10.1353/book2643

[27] DeVore, M.R. and Lee, S. (2017). APT(ADVANCED PERSISTENT THREAT)S AND INFLUENCE: CYBER WEAPONS AND THE CHANGING CALCULUS OF CONFLICT. *The Journal of East Asian Affairs*, [online] 31(1), pp.39–64. Available at: https://www.jstor.org/stable/44321272.

[28] Doucouliagos, H. and Ulubaşoğlu, M.A. (2008). Democracy and Economic Growth: A Meta-Analysis. *American Journal of Political Science*, [online] 52(1), pp.61–83. https://doi.org/10.1111/j.1540-5907.2007.00299.x

[29] du Prel, J.-B., Röhrig, B., Hommel, G. and Blettner, M. (2010). Choosing Statistical Tests. *Deutsches Aerzteblatt Online*, [online] 107(19). Doi:https://doi.org/10.3238/arztebl.2010.0343.

[30] Dunn Cavelty, M. (2018). Europe's cyber-power. *European Politics and Society*, 19(3), pp.304–320. doi:https://doi.org/10.1080/23745118.2018.1430718.

[31] European Repository of Cyber Incidents (2024). *Methodology*. [online] EuRepoC: European Repository of Cyber Incidents. Available at: https://eurepoc.eu/methodology/.

[32] European Repository of Cyber Incidents (EuRepoC (2024). Global Dataset of Cyber Incidents V.1.2. *Zenodo*. [online] doi:https://doi.org/10.5281/zenodo.11108195.

[33] Feo, M.D. and Martino, L. (2022). Public–private partnership (PPP) in the context of European Union policy initiatives on critical infrastructure protection (CIP) from cyber attacks. In: D. Noble, R. Keast, J. Tronda and R. Pinheiro, eds., *www.elgaronline.com*. [online] Edward Elgar Publishing, pp.54–79. Available at: https://www.elgaronline.com/edcollchap/edcoll/9781800889644/9781800889644.00014.xml.

[34] François Delerue (2020). *Cyber Operations and International Law*. [online] Cambridge University Press. Doi:https://doi.org/10.1017/9781108780605.

[35] Gannon, A. (2021). Planes, Trains, and Armored Mobiles: Introducing a Dataset of the Global Distribution of Military Capabilities (rDMC). *SSRN Electronic Journal*, (67). doi:https://doi.org/10.2139/ssrn.3930390.

[36] Giampiero Giacomello, Iovanella, A. and Martino, L. (2023). A Small World of Bad Guys: Investigating the Behavior of Hacker Groups in Cyber-Attacks. *arXiv (Cornell University)*. DOI:https://doi.org/10.48550/arxiv.2309.16442.

[37] Giegerich, B., Childs, N. and Hackett, J. (2018). *Military capability and international status*. [online] IISS. Available at: https://www.iiss.org/online-analysis/military-balance/2018/07/military-capability-and-international-status/.

[38] Gilli A. and Gilli M. (2019) *Why China Has Not Caught Up Yet: Military-Technological Superiority, Systems Integration, and the Challenges of Imitation, Reverse Engineering, and Cyber-Espionage*, *International Security*, Vol. 43, No. 3 (Winter 2018/19), pp. 141–189, https://doi.org/10.1162/isec_a_00337

[39] Guerrero-Saade, J. (2018). *Draw me like one of your French APTs – Expanding our descriptive palette for cyber threat actors*. [online] Available at: https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Guerrero-Saade.pdf.

[40] Guerrero-Saade, J.A. (2015). *The ethics and perils of APT research The ethics and perils of APT research: An unexpected transition into intelligence brokerage*. [online] Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20080228/Guerrero-Saade-VB2015.pdf.

[41] Haugaard, M. (2012). Rethinking the four dimensions of power: domination and empowerment. *Journal of Political Power*, 5(1), pp.33–54. doi:https://doi.org/10.1080/2158379x.2012.660810.

[42] Healey, J. (2024). *Cyber Effects in Warfare: Categorizing the Where, What, and Why - Texas National Security Review*. [online] Texas National Security Review. Available at: https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why/#article.

[43] Hunter, L.Y., Albert, C.D., Garrett, E. and Rutland, J. (2022). Democracy and cyberconflict: how regime type affects state-sponsored cyberattacks. *Journal of Cyber Policy*, 7(1), pp.72–94. doi:https://doi.org/10.1080/23738871.2022.2041060.

[44] Isaac Ben Israel and Lior Tabansky (2015). *Cybersecurity in Israel*. [online] Springer. Doi:https://doi.org/10.1007/978-3-319-18986-4.

[45] Iwińska, K., Kampas, A. and Longhurst, K. (2019). Interactions between Democracy and Environmental Quality: Toward a More Nuanced Understanding. *Sustainability*, 11(6), p.1728. doi:https://doi.org/10.3390/su11061728.

[46] J Andrés Gannon (2023). Planes, Trains, and Armored Mobiles: Introducing a Dataset of the Global Distribution of Military Capabilities. *International Studies Quarterly*, 67(4). doi:https://doi.org/10.1093/isq/sqad081.

[47] Katagiri, N. (2024). Advanced persistent threats and the 'big four': State-sponsored hackers in China, Iran, Russia, and North Korea in 2003–2021. *Comparative strategy*, pp.1–20. doi:https://doi.org/10.1080/01495933.2024.2317251.

[48] Klimburg, A. and Tirmaa-Klaar, H. (2011). *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. [online] Policycommons.net. Available at: https://policycommons.net/artifacts/1339311/cybersecurity-and-cyberpower/1948895/fragments/.

[49] Kose, J. (2021). *Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage*. [online] Available at: https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/journalpdfs/feature0421.pdf.

[50] Krebs, B. (2024). *BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare – Krebs on Security*. [online] Krebsonsecurity.com. Available at: https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/.

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

[52] Leslie, N.O., Harang, R.E., Knachel, L.P. and Kott, A. (2017). Statistical models for the number of successful cyber intrusions. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, [online] 15(1), pp.49–63. doi:https://doi.org/10.1177/1548512917715342.

[53] Levite, A. (2023). *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict*. [online] Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544.

[54] Lin, H. (2022). Russian Cyber Operations in the Invasion of Ukraine. *The Cyber Defense Review*, [online] 7(4), pp.31–46. Available at: https://www.jstor.org/stable/48703290.

[55] Liz Rivas, L. (2024).Violencia y agresión entre iguales a través de las TICS: Cyberbulling. AlmaMater. Cuadernos de Psicosociobiología de la Violencia: Educación y Prevención, nº 5, 2024, Dykinson, pp. 89-105. https://doi.org/10.14679/3314

[56] Liz Rivas, L. (2023). La agresión sexual en los conflictos prolongados. Derecho de intervenir y obligación de proteger. *Cuadernos de RES PUBLICA en derecho y criminología*, (1), 71–84. https://doi.org/10.46661/respublica.8044

[57] Luque Juárez, J. M., Payá Santos , C. A., & Arenas Morales, F. (2023). Contexto de las políticas de seguridad ciudadana. *Cuadernos de RES PUBLICA en derecho y criminología*, (2), 69–82. https://doi.org/10.46661/respublica.8293

[58] Mahoney, C.W. (2021). Corporate Hackers: Outsourcing US Cyber Capabilities. *Strategic Studies Quarterly - Perspective*, [online] 15(1). Available at: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15_Issue-1/Mahoney.pdf.

[59] Maness, R., Valeriano, B. and Jensen, B. (2019). *Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 1.5*. [online] Available at: http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf.

[60] Maness, R.C. (2019). A crisis of trust: Transatlantic cybersecurity relations in the post-Snowden era. In: G. Friedrichs, S. Harnisch and C.G. Thies, eds., *The Politics of Resilience and Transatlantic Order*. [online] London: Routledge, pp.190–209. https://doi.org/10.4324/9780429028847-9

[61] Martino, L. (2018). La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale. *Politica e Società*, [online] 1, pp.61–76. doi:https://doi.org/10.4476/89790.

[62] Martino, L. (2021). Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza. *IAI Papers*, [online] 21(13). Available at: https://www.iai.it/sites/default/files/iaip2113.pdf.

[63] Martino, L. (2023). La guerra nel XXI secolo: la dimensione cyber e il conflitto russo-ucraino. In: *La guerra tiepida: Il conflitto ucraino e il futuro dei rapporti tra Russia e Occidente*. Rome: Luiss University Press.

[64] Martino, L. (2024). Cybersecurity in Italy. Governance, Policies and Ecosystem. Springer Nature. https://doi.org/10.1007/978-3-031-64396-5

[65] Martino, L. (2024). International Law, State Sovereignty and Competition in the Digital Age. *Rivista di filosofia del diritto internazionale e della politica globale*, Vol. 21, Nº. 2, 2024. https://dialnet.unirioja.es/descarga/articulo/10098952.pdf

[66] Maschmeyer, L. (2024). *Subversion*. Oxford University Press. https://doi.org/10.1093/oso/9780197745854.001.0001

[67] Nazli Choucri (2012). *Cyberpolitics in International Relations: Context, Connectivity, and Content.* MIT Press.

[68] Nazli Choucri and Clark, D.D. (2018). *International relations in the cyber age : the co-evolution dilemma*. Cambridge, Ma: The Mit Press.

[69] Nye, J. (2010). *Cyber Power*. [online] Available at: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

[70] Olszewski, B. (2018). Advanced persistent threats as a manifestation of states' military activity in cyber space. *Scientific Journal of the Military University of Land Forces*, 189(3), pp.57–71. doi:https://doi.org/10.5604/01.3001.0012.6227.

[71] Oppenheimer, H. (2024). How the process of discovering cyberattacks biases our understanding of cybersecurity. *Journal of peace research*, 61(1), pp.28–43. doi:https://doi.org/10.1177/00223433231217687.

[72] Payá Santos, C. A, Delgado Morán, J. J;. Martino, L; García Segura, L, A.; Diz Casal, J, & Fernández Rodríguez, J, C. (2023). Fuzzy Logic analysis for managing Uncertain Situations. Review of Contemporary Philosophy Vol 22 (1), 2023 pp. 6780 -6797. https://doi.org/10.52783/rcp.1132

[73] Payá Santos, C. A, Delgado Morán, J. J. y Fernández Rodríguez, J. C. (2015) Los medios de producción de inteligencia, en el análisis actual de los conflictos, *Estudios en Seguridad y Defensa*, 10(20), pp. 5–17. doi: 10.25062/1900-8325.31.

[74] Payá Santos, C. A. (2023). El desempeño de la inteligencia en España en el ámbito público, empresarial y académico. *Revista Científica General José María Córdova*, *21*(44), 1029–1047. https://doi.org/10.21830/19006586.1222

[75] Pires, S. and Mascarenhas, C. (2023). Cyber Threat Analysis Using Pearson and Spearman Correlation Via Exploratory Data Analysis. In: *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC)*. [online] pp.257–262. doi:https://doi.org/10.1109/icsccc58608.2023.10176973.

[76] Recorded Future (2023). *North Korea's Cyber Strategy*. [online] Available at: https://go.recordedfuture.com/hubfs/reports/cta-nk-2023-0622.pdf.

[77] Rid, T. and Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), pp.4–37. doi:https://doi.org/10.1080/01402390.2014.977382.

[78] Robert Owen Keohane and Nye, J.S. (1977). *Power and interdependence*. London: Harpercollins, Cop.

[79] Robertson, R. (1992). *Globalisation: Social Theory and Global Culture*. London: Sage.

[80] Rodríguez González, V., Payá, Santos., C, A., & Peña Herrera. B. (2023). Estudio criminológico del ciberdelincuente y sus víctimas. *Cuadernos de RES PUBLICA en Derecho y criminología,* (1) 95-107. https://doi.org/10.46661/respublica.8072.

[81] Sanger, D.E. and Schmitt, E. (2015). Hackers Use Old Lure on Web to Help Syrian Government. *The New York Times*. [online] 2 Feb. Available at: https://www.nytimes.com/2015/02/02/world/middleeast/hackers-use-old-web-lure-to-aid-assad.html.

[82] Sanz González, R, Luque Juárez, J, M.ª, Martino, L, Liz Rivas, L, Delgado Morán, J. J. & Payá Santos, C. A. (2024) Artificial Intelligence Applications for Criminology and Police Sciences. *International Journal of Humanities and Social Science.* Vol. 14, No. 2, pp. 139-148. https://doi.org/10.15640/jehd.v14n2a14

[83] Shandler, R. and Canetti, D. (2024). Introduction: Cyber-conflict – Moving from speculation to investigation. *Journal of peace research*, 61(1). doi:https://doi.org/10.1177/00223433231219441.

[84] Singer, J.D., Stuckey, J. and Bremer, S.A. (2012). *Capability Distribution, Uncertainty, and Major Power War, 1820–1965 1*. [online] Routledge. Available at:

https://www.taylorfrancis.com/chapters/edit/10.4324/9780203128398-23/capability-distribution-uncertainty-major-power-war-1820%E2%80%931965-1-david-singer-stuart-bremer-john-stuckey.

[85] The Economist Intelligence Unit (2024). *Democracy Index 2023 Age of Conflict*. [online] London: EIU. Available at: https://www.eiu.com/n/campaigns/democracy-index-2023/.

[86] The International Institute for Strategic Studies (2021). *Cyber Capabilities and National Power: A Net Assessment*. [online] IISS. Available at: https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/.

[87] Tikk, E. (2020). What do we talk about when we talk about international cybersecurity. In: E. Tikk and M. Kerttunen, eds., *Routledge Handbook of International Cybersecurity*. [online] London: Routledge. Available at: https://doi.org/10.4324/9781351038904.

[88] Van Niekerk, B. (2018). *Information warfare as a continuation of politics: An analysis of cyber incidents*. [online] IEEE Xplore. Doi:https://doi.org/10.1109/ICTAS.2018.8368758.

[89] Vijayan, J. (2024). *Russian APT Releases More Deadly Variant of AcidRain Wiper Malware*. [online] www.darkreading.com. Available at: https://www.darkreading.com/cyberattacks-data-breaches/russian-apt-releases-more-deadly-variant-of-acidrain-wiper-malware.

[90] Voo, J., Hemani I. and Cassidy, D. (2023). National Cyber Power Index 2022. Belfer Center for Science and International Affairs, Harvard Kennedy School

[91] Whyte, C. (2020). Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online. *European Journal of International Security*, 5(2), pp.195–214. doi:https://doi.org/10.1017/eis.2020.2.

[92] Wilusz, D., Sadowczyk, D., Wójtowicz, A. and Tasiemski, L. (2022). *Long Tail of Security Vulnerabilities and Nation State APT Actors*. [online] Available at: https://www.kti.ue.poznan.pl/sites/default/files/SECS_2022_Long_tail_manuscript.pdf.

Notes

[i] Data was pre-processed to handle missing values and normalised where necessary. Statistical analyses were performed using Python, ensuring accurate computation and interpretation of results. Results were interpreted based on conventional significance levels (e.g., $p < 0.05$). For regressions analysis, the significance of the slope and the pseudo-R-squared value were key indicators, while for correlation and comparative tests, p-values determined the significance of the findings.

[ii] For research purposes, the same analysis conducted using The Economist's Democracy Index was also performed with Polity V. While the majority of countries retained similar classifications as authoritarian, hybrid, or democratic regimes, a notable discrepancy was observed in the case of Russia, which Polity V identified as a hybrid regime. This discrepancy does not indicate a flaw in Polity V but highlights the limitations of its most recent data, which is from 2018 and thus does not account for the internal consequences of the war in Ukraine. Even when using a 10-year average, covering 94. 95% of cyberattacks, Polity V data presents challenges for current research in topics with a fast-changing dynamics, underscoring the need for more recent indices like The Economist's Democracy Index.

Figures

Figure 1

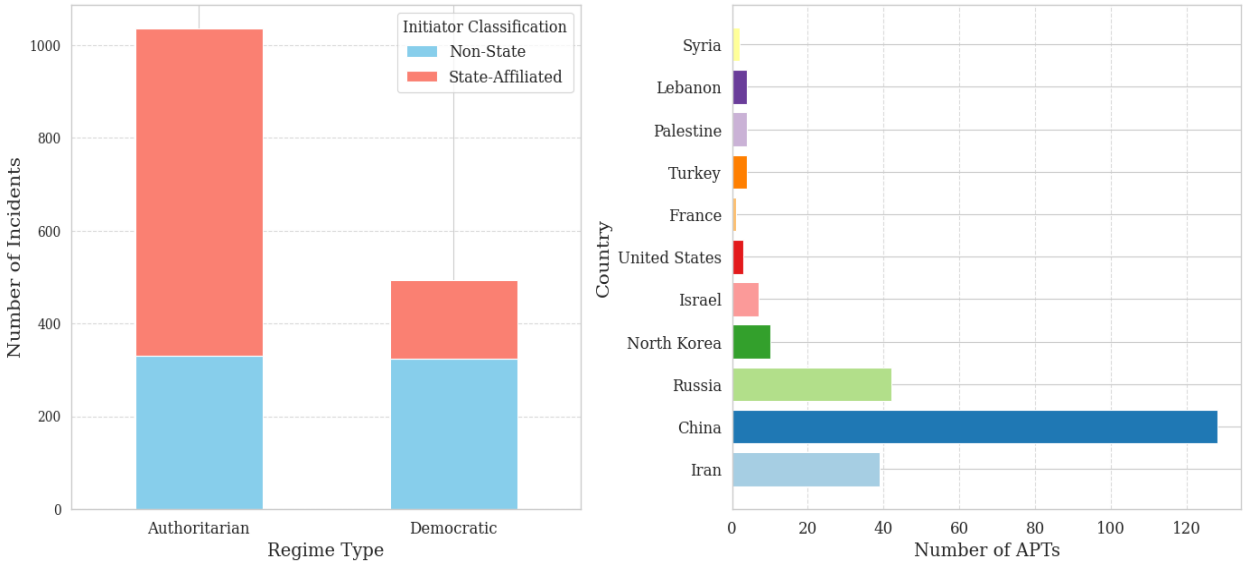


Figure 2

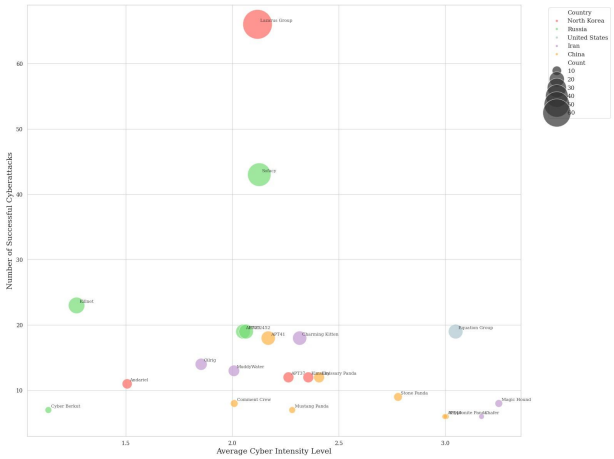
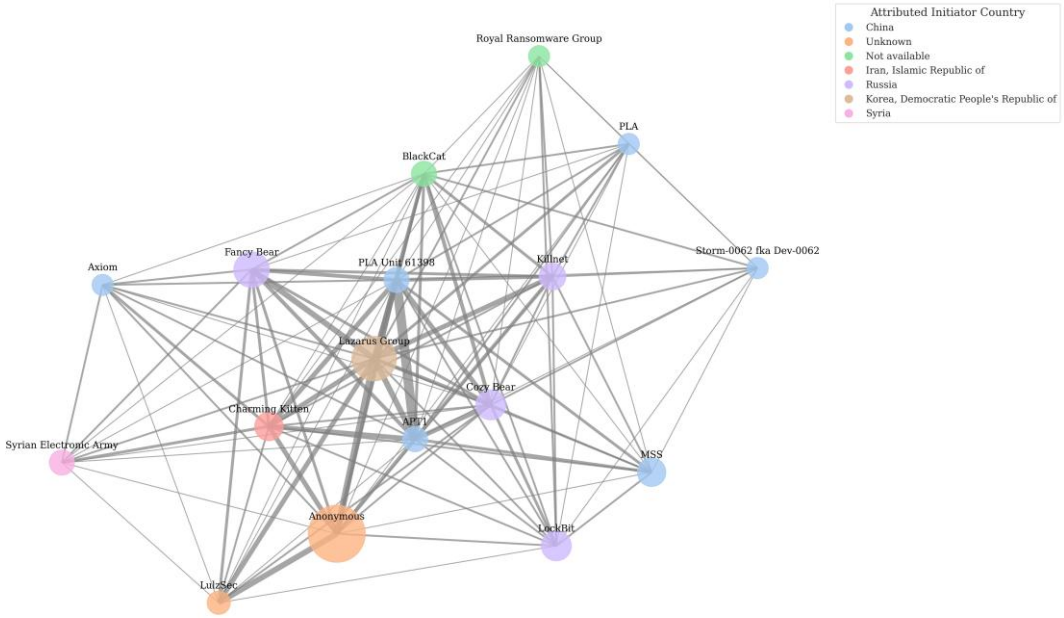


Figure 3


Attributed Initiator Country
China
Unknown
Not available
Iran, Islamic Republic of
Russia
Korea, Democratic People's Republic of
Syria
Royal Ransomware Group
PLA
BlackCat
Fancy Bear
PLA Unit 61398
Killnet
Storm-0062 fka Dev-0062
Axiom
Lazarus Group
Cozy Bear
Charming Kitten
APT1
Syrian Electronic Army
MSS
Anonymous
LockBit
LulzSec