Typology of State Actors' Behavior in Cyber Space

Ada Peter and Ujunwa Ohakpougwu
Communications Department, Covenant University, Nigeria

ada.peter@covenantuniversity.edu.ng;
ado909@g.harvard.edu
ujunwa.ohakpougwupgs@stu.cu.edu.ng

Abstract: Cyberwar is no longer subject to "if" but "when." Despite growing interest in cyberspace and cyber war readiness and resilience among academics, researchers, policymakers, and the media, the area needs to be more robust with different terminology that strategically captures the activities of state actors in cyberspace. The paper aims to provide a strategic classification of the activities of state actors in cyberspace. A typology is developed to encapsulate the strategic complexity of the activities of state actors in this terrain. The typology can illuminate the current global proportion and payoff of each type.

Keywords: Cyber, Cyber war, State actors, Behavior, Strategy, Cyberspace, Replicator dynamics

1. Background

We have intercepted a code that looks like it may be designed to be triggered in the next few weeks – basically during the swearing-in period for the United States Congress and state governments across the country, including the white house and Capitol Hill, and precisely January 3 when Vice President Kamala Harris will be administering the oath of office. Wondering why? Russia is seeking a sizable retaliation point for massive U.S. support to Ukraine which led to its recent withdrawal from Kherson. Russians think the best way to send this message and disrupt the government at critical moments in Washington and across the states is to turn out the lights and hamper the transition period requiring the focus of Washington, D.H.S., and maybe D.O.D. Who knows what they will try to pull on U.S. allies?

The situation above is entirely fictional, but the events are drawn from headlines and current affairs to reflect that in cyberspace, the probability of warfare through the fifth domain has shifted from questions of "if cyberwarfare occurs" to questions of "when cyberwarfare occurs." Hence there are research attempts to examine how cyberspace evolved from an intelligence tool to a destructive weapon targeted at critical infrastructures (Peter & Ohakpougwu, 2023). There are also several efforts to measure how well state actors are preparing, prepared, or at risk (Jegede, 2019 et.al; Peter & Sobowale, 2015.) These existing assessments estimate and evaluate the cyber power and, by extension, the cyberwar readiness of state actors.

Among several assessments, the World Economic Forum's 2016 *guesstimation* suggests that the United States, China, Russia, Israel, and the United Kingdom had the most developed cyber warfare capabilities. The International Telecommunication Union (I.T.U.) Global Cybersecurity Index (GCI), which assesses the commitment of member states to cyber security along five pillars, rates the United States, United Kingdom, France, Russia, and China's performance between 80% -100%, with the U.S., rated 100% (I.T.U., 2014,2017,2018, 2020). The Cyber Resilience Preparedness Index (C.R.I.), published in 2017, zoomed in on Africa's top 12 emerging economies. Egypt, Nigeria, and Kenya were classified as the most cyber-resilient countries on the continent (Peter, 2017). The Belfer Center's National Cyber Power Index (NCPI) at the Harvard Kennedy School considered cyber power in the context of seven national objectives countries pursue using cyber means (Voo *et al.,* 2020). Again, the United States, the United Kingdom, China, the Netherlands, Russia, and France were ranked the top six countries with the highest cyber power. Another measure worthy of note is the International Institute for strategic studies (IISS) qualitative assessment of 15 countries' cyber power. The only country classified as a tier 1 country on the IISS assessment is the United States. The United Kingdom, France, Russia, China, Iran, and DPRK were classified as tier 2 countries (IISS 2021).

At first glance, the position of high-ranking countries on each assessment subtly projects a false sense of cyberwar preparedness, readiness, and resilience to the intent and capabilities of cyber adversaries. However, state actors resting or acting on their GCI, IISS, C.R.I., and NCPI performance can be likened to ticking off as available all the weapons necessary in the outbreak of war without reflecting on how well weapons will or should perform in the face of adversity or a more sophisticated weapon. Also, the various cyber power indices must provide high-level defense decision-makers with appropriate information for assessing cyberwar readiness. For instance, countries like the United States, United Kingdom, France, Russia, and Germany, which rank 98%-100% on the GCI, can neither rest nor double their efforts based on their GCI ranking. The reason is that neither

nation's high or low commitment reflects cyber adversaries' interest or capacity to launch cyberattacks on a country's cyber infrastructure. Also, though the United States, United Kingdom, France, Russia, and Germany rank 98%-100% on the GCI, critical infrastructures belonging to these top-ranked countries remain at risk. Compromise, espionage, malware, ransomware, and attacks on industrial control systems continue to increase because cyber warfare tools, tactics, and procedures (TTP) evolve so quickly that cyber power and capability measures based on cyber defense legislation and law enforcement remain behind the activity curves of state and non-state attackers.

Hence, a replicator dynamic behavior model for assessing a nation's cyberwar readiness and resilience may be a more helpful framework for state actors to track each actor's cyber resilience, cyberwar readiness, and possible future behavior. However, to develop a cyber replicator dynamic equation of state behaviors in cyberspace, the research requires three critical pieces of data. First is some type of behavior in cyberspace, next is the proportion of each type, then the payoff for each type of cyber behavior within and between state actors.

The current paper, therefore, focuses on classifying the varying means or processes by which nations prepare and pursue cyber warfare across 16 critical infrastructures dependent on cyberspace. Typologies are critical for three reasons. The first is to encapsulate the strategic complexity of the activities and behavior of state actors in cyber terrain. Second, it serves as a precursor for illuminating each type's current global proportion and payoff, which are necessary to examine future evolutionary dynamics. Moreover, as a valuable tool for indexing, a typology of state actors' behavior in cyberspace holds insights into each type of state activity's evolutionary possibilities. It provides opportunities for close strategic case studies of individual state actors' behavior in cyberspace.

Subsequent papers report the procedures for identifying the proportions of each type, the payoffs, and an index of each nation's performance based on each type. With data on these critical aspects, the feasibility of a dynamic replicator model of state actors' behavior in cyberspace increases so that decision-makers can step away from dominantly reactive cyber strategies to proactive approaches.

2. Method

To create the typology of state actors' behavior in cyberspace, the research adopts Yin's cross-case/multiple-case studies approach to examine multiple cases of state-backed cyber-attacks. The design for developing a typology of state actors' practices in cyberspace is based on a replication logic. According to Yin, reliance on theoretical concepts remains one of the essential strategies for completing successful case studies, whether exploratory, descriptive, or explanatory (Yin, 2017). These include the development of preliminary concepts at the outset of a case study, placing it within the appropriate research literature defining the units of analysis, identifying criteria for selecting and screening potential cases, and suggesting variables of interest. Donella Meadows's systems theory also provides the theoretical framework guiding the questions used to cross-examine each case (Meadows, 2008). The theory suggests that the behavior of state actors in cyberspace can only be understood by studying trends over time rather than focusing attention on individual events. At a 90% confidence level, the researcher selected 32 out of 776 state-backed attackers executed by the top five state actors responsible for 84% of all the attacks between 2005 and 2021 (See Figure 1). The top five state actors responsible for 84% of all attacks include the United States, Russia, China, North Korea, and Iran. The criteria for selecting the cases are

- One of these five countries (United States, Russia, China, North Korea, and Iran) executed the attack on another state actor between 2005 and 2021
- The attacks with the longest recovery time executed by these countries
- The attacks must be on cyber-dependent critical infrastructures that support the functions of other critical infrastructures.

The study excludes the behavior of state actors in contexts of authorized access for intelligence gathering and sharing like those that exist among the five or seven eyes.

It is also important to note that 85% of these attacks occurred between countries experiencing tense or sour political, economic, and social relations at the time of the attack. Most US-reported cyber-attacks were towards Russia, Iran, and North Korea.

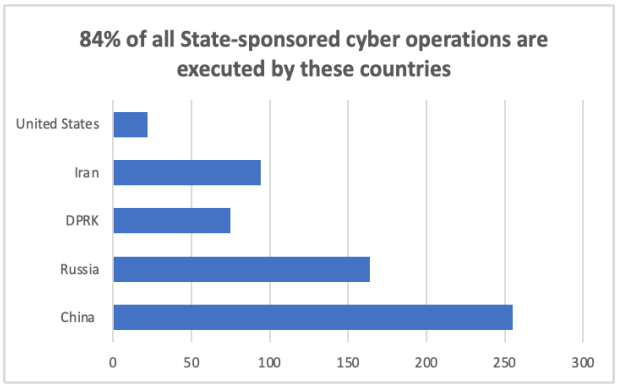

Figure 1: Five State Actors responsible for 85% of State-backed Disruptions in Cyberspace

Based on these criteria, 5% of the attacks with the most significant impact on critical infrastructure and severity executed by these countries were selected. Impact and severity were measured by how many critical sectors depended on the affected sector, the recovery time, and the financial loss. Analysis of 16 cyber-dependent critical sectors by Peter (2022) reveals that some sectors are more dependent on other sectors (See figure 2), so a successful attack on a sector with many dependencies yields greater rewards for the attacker. The longer the time it takes to recover, the higher the severity. The research objects for the study were the targeted cyber-dependent critical infrastructures associated with it political, social, and historical relevance and or issues.

Country	Target Rate	Cases studied
China	255	13
Russia	164	8
DPRK	75	4
Iran	94	5
United States	22	2

We then conducted a traditional cross-case analysis of 32 cases of state-backed attacks collected from the Council on Foreign Relations data on state-sponsored cyber operations (https://www.cfr.org/cyber-operations). Famous examples of the 32 cases selected include Stuxnet; the Microsoft Exchange server attack, which affected the European Banking Authority and other organizations globally; the SONY hack; the U.S. Colonial Pipelines, the Russian electric grid; the SolarWinds attack, etc**.** The following key questions were used to examine each case.

- What critical infrastructure was attacked? EXECUTE
- Does the attack share common conditions with other attacks?
- What are the shared common and uncommon conditions?
- Which communication or information technology aided the attack? (Satellite, Network services, Network hardware products, cloud services, cybersecurity tools, social networks, internet) FARMING
- At the time of the attack, what was the state of the communication/I.T. infrastructure that aided the attack? A home or foreign-owned Communication and I.T. infrastructure? (FARMING)
- How did the attack work? (EXPLOIT)
- What actions did the various actors take (hero and villain) before and after the attack? -DEV/PATCH
- What is the geographical reach of the communication/I.T. infrastructure that aided the attack?
- Has the communication/I.T. infrastructure that aided the attack been updated in the past?
- What are the diplomatic relations between the hero and the villain? (Economic, social, intelligence sharing, and political)

The researcher also reviewed several contents and synthesized empirical findings, public debates, and reports mentioning state actors. These include N.S.A. leaked documents, proceedings of vulnerability conferences

(DEFCON, BruCON, Black Hat Europe, Cold Blue, Null CON, Zero Nights, 44CON), vulnerability reports, exploit reports, patches, and the CISA database. The review focused only on state actors' offensive and defensive activities across 16 cyber-dependent critical infrastructure sectors (See figure 2), including Chemical, Commercial, Communication, Defense Industrial Base, Dams, Energy, Emergency Services, Financial, Food and Agriculture, Government Facilities, Health and Public Health, Information Technology, Critical Manufacturing, Nuclear, Transportation, Water, and Wastewater Sectors.

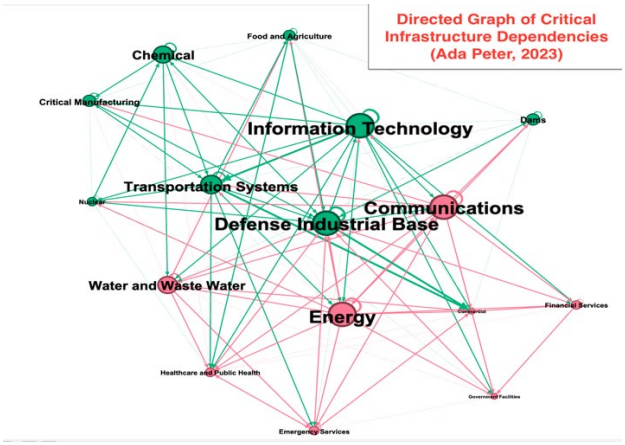

Figure 2: Directed Graph of Critical Infrastructure Dependencies (Ada Peter, 2023)

The figure represents 16 critical infrastructure sectors (nodes) of cyber-dependent States. Arrows pointing to a node show the sectors depending on it and vice versa. The larger nodes (e.g., defense industrial sector) indicate that more sectors depend on that node than the smaller nodes (e.g., chemical sector). Thus, a targeted disruption or destruction of the larger nodes will have ripple effects on all the dependent sectors, generating a higher impact than an attack on the smaller nodes. The larger the node, the higher the risks; thus, decentralizing critical infrastructure dependency within and between sectors may enhance cyber resilience outcomes.

The preceding data analysis broadly revealed six means or processes by which nations prepare and pursue cyber warfare across 16 critical infrastructure sectors (See Figure 2) dependent on six critical areas of communication and information technology. The means and processes identified and classified include

- Farming vulnerabilities
- Unearthing vulnerabilities
- Developing payload exploits
- Executing exploits
- Storing arsenals of allies' and enemies' vulnerabilities and possible exploits
- Patching vulnerabilities

Farming Vulnerability (F.V.): State actors understudy were found to use the spread of homemade and foreign technologies as a cyberweapon. F.V. appears both as an offensive and defensive posture. F.V., on the one hand, gives the home country offensive access to foreign data and, on the other hand, offers offshore countries the opportunity to gain access to the home country's network services, equipment, intellectual property, how it works, understand the vulnerabilities, and build ready-to-deploy exploits. F.V. is the necessary means by which state actors pursue cyber war. Peter & Ohakpougwu's (2023) assessment of how the internet gets weaponized, indicates that farming vulnerability occurs across all the stages of weaponization, excluding cyber-independent phase of cyber weaponization.

Farming refers to the spread of state actors' information and communication technology services and products, including cloud security, network services, and equipment, satellite services and equipment, and internet services and equipment to other countries and continents. Examples include backbone I.S.P.s such as Backbone I.S.P.s (AT&T, CenturyLink, Cogent Communications, Deutsche Telekom, Global Telecom and Technology (GTT), N.T.T. Communications, Sprint, Tata Communications, Telecom Italia Sparkle, Telia Carrier, and Verizon), Cloud service (Amazon Web Services (A.W.S.), Microsoft Azure, Google Cloud Platform (GCP), Alibaba Cloud, Oracle Cloud, I.B.M. Cloud (Kyndryl), Tencent Cloud, OVHcloud, DigitalOcean, and Linode (owned by Akamai)—hardware and software companies like Apple, Google, Weibo, WeChat, TikTok, Huawei, etc.

Unearthing Vulnerabilities (U.V.): The country's understudy has commissioned teams whose singular goal is to unearth internal and external vulnerabilities. U.V. is both an offensive and defensive posture. U.V. refers to countries coordinating the daily activity of finding their vulnerabilities and external vulnerabilities of on-shore and offshore software and hardware network services and equipment, cloud security, internet services, and satellites used across its critical infrastructure sectors, including Chemical, Communication, Commercial Defense industrial base, Energy, Finance, Government facilities, Health and public health services, Information technology, Manufacturing, Nuclear, Transportation, Water, and wastewater. For instance, the primary purpose of the United States' Common Vulnerabilities and Exposures (C.V.E.) The program identifies vulnerabilities uniquely and associates specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities. China's version of the US NVD is the **Chinese National Vulnerability Database** (**CNNVD**). It is the national vulnerability database that catalogs all software defects and patches. In the cyber weaponization process, countries are only capable of unearthing vulnerability particularly in building resilient critical infrastructure phase (Peter & Ohakpougwu, 2023).

Developing Exploits (DEVEX): State actors also develop exploits. For adversarial state actors, finding or unearthing vulnerabilities is worthless without payloads to exploit those vulnerabilities. While finding vulnerabilities are worthful for adversaries with payloads to exploit those vulnerabilities, on the flip side, exploits are worthless for the adversaries when those vulnerabilities are quickly patched. Hence, state actors step beyond identifying common application vulnerabilities to developing exploits that penetration testing may not capture. Publicly available examples of state-backed efforts to develop exploits are ethical hackers, more intrusive and involve active exploitation of security vulnerabilities. The Cybersecurity and Infrastructure Security Agency (CISA), a federal agency of the U.S. government, recently selected Bug Crowd to launch its first federal civilian enterprise-wide crowdsourced vulnerability disclosure policy (V.D.P.) platform. The V.D.P. platform enables agencies to identify and monitor vulnerabilities in critical systems by receiving security feedback from uniquely skilled ethical hackers worldwide. Two critical cycles must be completed for these ethical hackers to provide feedback. First, identify the vulnerabilities, and second, exploit the vulnerabilities. N.S.A. leaked documents also reveal how the United States exploits vulnerabilities for military, economic, or political motives. More so, intelligence gathering and espionage via digital means are impossible without state actors using developed exploits to gain access back door access to information. While several nations are engaging DevEx, as Table One indicates, China develops payloads for exploiting known and unknown vulnerabilities.

Executing Exploits (EXEX): The countries' understudy has executed detrimental exploits at different times. These are the most common, repeated, and reported means of pursuing cyber warfare. As an offensive posture, executing exploits include state-backed attacks on the digital infrastructure of other countries. Several state actors in North America, Asia and Europe have shown traits of these behavior. Examples include the 2022 disruption of U.S. gas pipelines, Russia's alleged use of social media campaign to interfere in the 2016 U.S. presidential elections, the late 2014 North Korean attack on Sony Pictures in connection to a planned release of the poorly reviewed movie, *the interview,* the 2010 American Stuxnet attack on Iran and North Koreas weapon's program and the Chinese decades-long espionage of U.S. trade secrets including those extracted *from the* Booz Allan Hamilton, Russian disruption of 2016 U.S. elections, and the Chinese-backed attack on the European banking authority. These attacks are simply apparent execution of identified vulnerabilities and developed exploits. The benefits and gains can range from the show of cyber power to political, military, economic, and diplomatic benefits. The Centre for Foreign Relations tracks reports of this type of state-backed attacks. Unlike other continents, state actors in Africa, have no records of executing disruptive exploits (Peter & Sobowale, 2015). Non execution of exploits also suggests that state actors in Africa may be lagging around the pre-cyber dependent critical infrastructure phase (Peter & Ohakpougwu, 2023).

Patching (P): State actors commission patches of vulnerable cyber tools. Patching is a defensive posture. It is essential to coordinate vulnerability disclosure, especially for public-facing digital infrastructure. It refers to fixing vulnerabilities identified within a digital infrastructure as soon as possible. State actors with patching standards and laws are better defenders of their digital infrastructure since patches incapacitate payloads configured to exploit known-known and known-unknown vulnerabilities.

Storing Vulnerabilities and Exploits (SVEX): Countries store vulnerabilities and exploits. Storing vulnerabilities, especially zero-day vulnerabilities, can be likened to storing a war arsenal that will be deployed when needed. However, since storing vulnerabilities and exploits to pursue cyber warfare is highly correlated to farming and unearthing, DEVEX, and EXEX, the model assumes that countries that rank above average for all five certainly store or stockpile zero-day vulnerabilities. Zero-day stockpiles are treasures unearthed and stored for valuable times. Governments' use of zero-day exploits has exploded over the last decade, feeding a lucrative market for

defense contractors and others who uncover critical flaws in the software (and hardware) and sell information about these vulnerabilities to their government customers. For example, the infamous Stuxnet, a digital weapon used to attack Iran's uranium enrichment program, used four zero-day exploits. While many state actors in Asia, Europe, Australia and North America have and continue to exhibit the behavior of storing arsenals, the tendencies of state actors in Africa to do same is not unclear since some state actors on the continent are gradually approaching the full spectrum of a cyber dependence (Peter & Sobowale, 2015).

3. Preliminary Conclusion

The preceding six means or processes by which nations prepare and pursue cyber warfare across 16 critical infrastructures dependent on cyberspace will constitute the basis for developing a dynamic replicator model accessing the evolution and performance of each state across each means. We hypothesize that state actors involved in all six means in an evolving approach are cyber-war-ready, while state actors passively or actively involved in some but not all means are in cyber-war readiness momentum, others without a trait of these activities are unprepared, their network readiness ranking notwithstanding.

Acknowledgement

We recognize the conference participation support from Covenant University

References

44CON https://44con.com Accessed November 16, 2022

Black Hat Europe https://www.blackhat.com/eu-22/ Accessed November 16, 2022

BRUCON https://www.brucon.org/2022/ Accessed November 16, 2022

Council on Foreign Relations Cyber Operations Tracker (2022). https://www.cfr.org/cyber-operations Accessed September 25, 2022

Cybersecurity and Infrastructure Security Agency (CISA) https://www.cisa.gov Accessed October 5, 2022

DEF CON (2022). https://defcon.org Accessed November 16, 2022

Donella Meadows (2008). Thinking in Systems. Chelsea Green Publishing

International Institute for Strategic Studies. Cyber Capabilities and National Power: A Net Assessment (2021). https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

I.T.U. (2014) https://www.itu.int/pub/D-STR-SECU-2015 Accessed September 5, 2022

I.T.U. (2017) https://www.itu.int/pub/D-STR-GCI.01-2017 Accessed September 5, 2022

I.T.U.(2018)https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf Accessed September 5, 2022

I.T.U. (2020) https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx Accessed September 5, 2022

Jegede, A., Okorie, N., Oyero, O., & Olowolafe O. (2019). Post humanism, Virtual Warfare, and the Defence Preparedness of Nations: A case for Africa's readiness.
(2019) *African Renaissance*, 16 (3), pp. 67-90.

Julia Voo, Irfan Hemani ,Simon Jones, Winnona DeSombre, Daniel Cassidy, Anina Schwarzenbach. National Cyber Power Index 2020 Methodology and Analytical Considerations (2020). https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf Accessed September 5, 2022

Marco De Falco (2012). https://ccdcoe.org/library/publications/?search=Stuxnet October 5, 2022

NIST (2022) National Vulnerability Database. https://nvd.nist.gov Accessed September 5, 2022

Peter, A. (2017). Cyber Resilience Preparedness of Africa's Top Emerging Economies (June 10, 2017). International Journal of Critical Infrastructure Protection, Vol.17 49-59

Peter, A. & Ohakpougwu, U. (2023). Origins of Cyberwarfare: How the Internet got Weaponized. (2023) *Proceedings of the 10th European Conference on Social Media, ECSM 2023*, pp. 364-372

Peter, A., Sobowale, I. (2015). Proceedings of the 25th International Business Information Management Association Conference - Innovation Vision 2020: From Regional Development Sustainability to Global Economic Growth, IBIMA 2015, 2015, pp. 73–86

Robert Yin (2017). Case Study Research and Applications Design and Methods. Sage Publications