Which Cyber Actor will be the Biggest Threat in the Next 5 Years?

James Read

College of Cybersecurity
Old Dominion University
jread001@odu.edu
4/20/2022

Problem Definition:

Computing and computer networks are integrated into nearly every aspect of government and corporate operations. A rapid rate of expansion and integration combined with a lack of foresight has prevented information security from keeping pace. The widespread vulnerability of computer networks now provides malicious actors with an inexpensive and relatively low risk means of conducting a wide range of attacks. This low barrier for entry attracts actors from a wide range of skill levels, means, and intent; resulting in an highly varied and complex threat landscape.

The ability to conduct these offensive operations far outpaces the capability to defend against them. Limited defensive resources and capabilities must be directed to where they are needed most. To accomplish this we need to identify the which actors pose the greatest threats. Such an analysis must also be forward looking, considering not just the current threat but the future as well. Among these actors one will foremost. *The question of which threat actor will pose the greatest threat in the next 5 years is the question that concerns this paper.*

To find the answer we can begin by conducting an overview of the current threat actor landscape. Most threat actors will fall into one of the following 7 categories. (1)

Script kiddies: Low skilled actors making use of off the shelf tools and scripts to attack their targets.

Black hat hackers: Malicious individuals with medium to high level skill sets targeting systems for a variety of personal motivations.

Hacktivists: Individuals and groups employing cyberattacks as activism. Motivated by a sense of social/ideological justice

Terrorists: Extensions of violent terrorist groups using cyberspace to recruit, train, share information, and organize real world attacks.

Organized *crime/cybercriminals*: Actors perpetrating traditional criminal acts such as drug and firearm dealers, production and distribution of child abuse material, financial fraud, human trafficking. Cybercrime also includes the high profile explosion of ransomware as a highly successful extortion technique.

Nation states: Nation sponsored actors employing cyber capabilities to engage in espionage, cyber crime, influence campaigns, suppress social and political dissent, and conduct direct attacks against adversaries.

Among these, organized cybercriminals and nation state actors are unique in the scale of their operations.

Cybercrime is expected to have a global cost of ~6 trillion U.S. dollars and estimated to climb to 10.6 trillion by 2025. (2) This would make it the world's third-largest economy after the U.S. and China. (2) Ransomware in particular has been devastating globally. It affects governments at every level, companies in all sectors. hospitals, and critical infrastructure. Affected organizations may cease to function entirely until the ransom is payed and there is no guarantee that payment will result in unlocking the system.

Hostile state actors collect a significant chunk of the cybercrime pie while also conducting operations beyond the capabilities of even organized cybercriminals. Superior capabilities and resources allow states to execute sophisticated espionage campaigns to compromise state secrets and steal intellectual property. They may also conduct malign influence campaigns and election interference to cause political unrest. Many are capable of disrupting critical infrastructure to cripple an adversary. Some authoritarian nations also use the cyber realm to clamp down on free expression in a effort to control social and political activity.

Cyber operations at the state level elevate the threat beyond the criminal to the existential. With these capabilities hostile state actors are able to threaten global stability, societal and international norms, and free expression. It is for these reasons that it can be considered the category of actor that poses the largest threat.

Of course, there are many state actors. Now we must ask, which are the most significant? A survey of publications, including the the U.S. Intelligence community, shows a nearly unanimous assessment of this question. *China, Russia, Iran, and North Korea* are the most prolific and effective cyber threat actors at the state level. (3) These four nations consistently top the charts in the number of significant attacks conducted each year with a demonstrated history of high profile adversarial campaigns against the U.S. and its allies. (4) To identify which of these actors poses the greatest threat let us take a closer look at each.

Analysis:

North Korea

Strategic Goals:

The Office of the Director of National Intelligence (ODNI) assesses that the primary strategic goal of North Korea is to guarantee regime safety and longevity. (3) To accomplish this it is focused on expanding both its nuclear and conventional capabilities. (3) By expanding its ability to threaten its regional neighbors and the United States with devastating attacks North Korea hopes to deter any overt attempts at regime change.

Capabilities:

According to the ODNI, "North Korea's cyber program poses a growing espionage, theft, and attack threat."

Notably, it has the ability to target critical infrastructure and business networks in the United States, causing limited disruptions. (3) It also has a demonstrated willingness to take bold action that makes it a likely candidate for conducting surprise cyberattacks. (3)

North Korea is also unique in its emphasis on using cybercrime to generate revenue. (5) It is known to target both the financial and cryptocurrency sectors worldwide, stealing an estimated $2 billion in 2019. (6)

*Notable Attack***s:**

2022: TraderTraitor - Malware campaign targeting blockchain organisations and the cryptocurrency industry. (5)

2020: FASTCash - Malware campaign targeting banks' retail payment system infrastructure allowing ATM cash-outs. (5)

2017: Wannacry Ransomware - Ransomware attack that infected over 230,000 computers in a single day and and causes billions of dollars in damages. (7)

2014: Sony Pictures Attack - Retaliation for the film 'The Interview', a story about the fictional assassination of Kim Jong-il. Sony Pictures Entertainment lost lost approximately 70 percent of ts information systems and $35 million (8)

Summary:

North Korea's goals are local, focusing primarily on regime stability and influencing its immediate neighbors. It's capabilities are growing but restricted by the size of the country and the funding available for cyber operations (thus the emphasis on generating revenue). While a serious threat, North Korea's goals and capabilities are limited when compared the other nations in the top four.

Iran

Strategic Goals:

Iran seeks to expand its influence and project power in the Middle East while eroding U.S. influence in the region and minimizing threats to regime stability (9)

"It sees itself as locked in an existential struggle with the United States and its regional allies." (3) It is prepared to directly attack U.S. citizens, particularly those living in the Middle East, and may use proxies as well. (3) Iran is also pursuing a decades long goal of establishing networks in the U.S. itself. (3)

Capabilities:

Iran uses cyber to suppress certain social and political activity and to harm regional and international adversaries. It engages in "conventional offensive cyber activities ranging from website defacement, spear phishing, distributed denial-of-service attacks, and theft of personally identifiable information, to more advanced activities—including destructive malware, social media-driven influence operations, and, potentially, cyberattacks intended to cause physical consequences." (9)

The ODNI notes that Iran has the "expertise and willingness to conduct aggressive cyber operations". It demonstrated the capacity to attack critical infrastructure in a series of attacks on Israeli water facilities in 2020. (3) It also conducted influence operations targeting the 2020 U.S. presidential election and is expected to focus influence efforts on disinformation and anti-US content. (3)

Notable Attacks:

2022: MuddyWater - Iranian APT group and associated malware tools identified as part of cyber operations targeting government and private-sector organizations including telecommunications, defense, local government, and oil and natural gas. (9)

2021: Iranian APT actors identified targeting multiple U.S. and Australian critical infrastructure sectors. (9)

2021: Iranian APT actor identified targeting U.S. state websites to obtain voter registration data. (9)

2020: Pioneer Kitten group identified in APT campaign targeting VPN vulnerabilities affecting U.S. federal agencies and other U.S.-based networks. (9)

Summary:

While it many of its aims are similar to that of North Korea, Iran's sphere of influence is broader with more regional neighbors and greater impact. Its larger economy also means a larger offensive cyber program with increased experience and capability. Iran represents a step up from North Korea in its threat posture but still lacks the massive resources of Russia and China.

Russia

Strategic Goals:

Russia claims a sphere of influence over many former soviet states, seeking to dominate its "near-abroad" including Ukraine and other former soviet countries. (3) In engaging the U.S. it seeks recognition of this claim and agreement on mutual noninterference in domestic affairs. (3)

Russia does not desire a direct conflict with the U.S. but does believe the U.S. seeks to undermine it. It thinks the U.S. seeks to remove Vladimir Putin from power and to expand NATO to threaten its borders. From this belief it justifies conducting retaliatory acts. (3)

Capabilities:

Russia employs it's capabilities to harm regional and international adversaries, collect Intelligence, suppress certain social and political activity, steal intellectual property. (10)

It has a demonstrated sophistication in the full spectrum of of cyberattacks including abilities in cyber espionage, malign influence, election interference, disrupting critical infrastructure, and disrupting business operations.

It is known to target industries and organizations in the following sectors: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing (10)

Russia also provides a safe harbor for ransomware gangs and other cyber criminals provided they do not interfere with Russian interests.

Notable Attacks:

2022: Industroyer2 - GRU hacker group Sandworm infected a Ukrainian energy company with malware to disrupt the power grid but it was caught before the attack could be executed.

2022: - Indictments of three Russian FSB officers for intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies. (10)

2020: SolarWinds - A supply chain attack exposing numerous federal agencies and private companies to infiltration via the Sunburst backdoor.

2017: Notpetya - Ransomware attack originating as part of limited cyberwar against Ukraine. Escaped to affect companies worldwide.

2016: GRIZZLY STEPPE - Campaign to compromise and exploit networks and endpoints associated with the U.S. election. (10)

Summary:

Russia represents a significant step up from Iran and North Korea in the scope of its goals and it's cyber capabilities. Its seeks not just to influence its neighbors but to dominate them, sometimes militarily. Its influence goals are global, with interests intersecting in Asia, Europe, and the Middle East. It sees offensive cyber operations as a tool for deterrence, military action, and foreign policy in support of these interests. (3) With the resources at its disposal, Russia has developed mature capabilities in the full spectrum of cyberwarfare.

China

Strategic Goals:

China's primary goal is become not just the preeminent power in East Asia but the preeminent power in the world. To achieve this it believes it must foster norms that favor its authoritarian system and undercut U.S. influence (3)

Like Russia, China aggressively rejects NATO expansion. It believes this and other alliances preserve a cold war mentality that serves to hamper it's own growth. (12) As a result China also seeks to weaken Western partnerships in favor of what it describes as "true multilateralism." (12)

Capabilities:

China leverages cyber operations to assert its political and economic development objectives. It is capable of the full range of cyber threats with a particular emphasis on espionage, cyberattack, and malign influence capabilities. It targets nearly every public and private sector including: healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms. (11)

China notably places a heavy focus on achieving an informational advantage on the world stage. To achieve this it conducts extensive operations to steal intellectual property in technology sectors and from critical infrastructure organizations. (11) This focus on espionage provides its firms with a competitive advantage and supports its expansion of technology-driven authoritarianism. (3)

Also of note is China's extensive use of surveillance and censorship. It monitors it's population to repress dissent and also targets foreign nationals, such as journalists, whom it perceives as threats. It has even used global Covid-19 cooperation to disseminate surveillance tools. (3)

Lastly, China is known to be expanding influence campaigns around the world to "promote its policy preferences, mold public discourse, pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China on such issues as religious freedom and the suppression of democracy in Hong Kong " (3)

Notable Attacks:

2021: Members of APT group APT40 indicted for theft of trade secrets, intellectual property, and other high-value information in the United States and abroad. (11)

2021: Microsoft Exchange Exploitation - Actors associated with PRC observed exploiting widespread vulnerabilities in Microsoft Exchange Server to install webshells. (11)

2015: OPM Breach - 22.1 million records affected including those of government employees other people who had undergone background checks, and their friends and family.

2007: F35 plans stolen - Supply chain attack targeting a Lockheed Martin subcontractor resulting in a data breach theft of sensitive IP including plans for the F35.

Summary:

China seeks to become the preeminent power on the world stage. It is the best at the methods that support those goals. It has superior cyber espionage capabilities because it is placing a premium on IP theft and intelligence gathering. It also makes the greatest use of authoritarian tools to crack down on dissent and surveil perceived threats at home and abroad. A growing ability to conduct influence campaigns helps it minimize the negative impact of these tactics and shape the global discourse in its favor.

Findings:

So who is the biggest threat actor? The answer is dependent on the criteria we are using. Are we concerned purely with monetary damage? What about loss of life? What other factors are there to consider?

It is extremely difficulty to find reliable, comparable statistics on the costs of cyberattacks. Available studies date from many different years and use many different measures. Many incidents are not even reported. The rapid escalation of cyberattacks annually combined with the lack of consistent metrics and gaps in data place an accurate comparison between actors beyond the scope of this paper.

Measures of loss of life present similar difficulties. Hospital ransomware certainly puts lives at risk, but how many? Activists are exposed and sometimes killed as a result of hacking and surveillance tools, but how often? The Russian war against Ukraine is costing a staggering number of lives and cyberattacks contribute to the war effort but how much do they contribute to the direct loss of life? What about indirectly? Very little data exists for these questions.

On what basis then can we grade the threats that these actors pose? I suggest a comparison of strategic goals and relative attack capabilities. Each of these countries has access the the same methods. Espionage, cybercrime, cyberattack, influence campaigns, social repression, and so on. The difference then is in the impact of their goals and sophistication of their capabilities.

Russia and China are the standouts in both categories. Their size and resources put them in a higher tier altogether than Iran and North Korea. Comparing the two, China's goals have a larger potential impact than Russia. Russia primarily seeks to establish and maintain a hold on it's perceived sphere of influence. China seeks to shift the entire geopolitical balance and place itself at the top. In the measure of capabilities, each is capable of the full spectrum of offensive cyber and each excels in the methods that best support their goals.

With that in mind, I submit that China is the biggest threat because it has the *most disruptive goals* and the superior capabilities to enact those goals. It seeks to challenge and replace U.S. influence globally and foster norms that favor its authoritarian system. It possesses the technological and economic power to do so.

China has the most active and persistent cyber espionage abilities of any adversary and they are actively and effectively using those capabilities to advance their goals. According to the ODNI, China is "the top threat to U.S. technological competitiveness as Beijing targets key sectors and proprietary commercial and military technology from U.S. and allied companies and institutions." The aggressive use of these capabilities undermines U.S. competitive advantages and "advances Beijing's ability to assume leadership of the world's technological advancement and standards." (3)

In that leadership lies the real threat. The competition between China and the U.S. is ideological. Self governance and free expression vs. censorship and authoritarian rule.. A dominant China means the spread of censorship and authoritarian rule as global norm, leveraged through technological and economic advantage. Therefore China will the biggest cyber threat actor over the next 5 years.

Recommendations:

Diplomacy

Recent agreements with China to set norms for cyber espionage and curb IP theft have correlated with a reduction in the amount of China attributed theft. Whether more gains can be made and if it will respect such norms in the long term seem questionable given its history, Still, the diplomatic dorr should be left open and further agreements should pursued to the extent China is not demonstrably negotiating in bad faith.

Policy

Economic sanctions are often seen as questionable in their effectiveness and Western reliance on cheap Chinese manufacturing leaves the U.S. open to retaliation. Still, they do have an impact and can occupy a middle ground between allowing China to conduct cyberattacks free of consequence and more aggressive action.

Cyber Defense

Its is well known that there is a personnel shortage in cyber security field across all sectors. Every effort needs to be made to close this gap and to tighten security across sectors.

Defend Forward

U.S. Cyber Command advocates a strategy of Defending Forward through a doctrine of Persistent Engagement. Its posits that we are already under cyber attack by our adversaries and should take offensive action close their point of origin to counter them. That not doing so cedes the advantage in a conflict that is already initiated.

The advantage to this approach is that it compels the adversary to shift resources to defense, creates freedom to maneuver in the cyber battlespace, and imposes costs on the enemy. (14)

The disadvantage is that it risks escalating cyber conflict and sets a norm of persistent offense.

Head of USCYBERCOM General Paul M. Nakasone claims that "Our restraint back in the day was escalatory in itself." He further justifies this doctrine stating, "They don't fear us. The longer that we have inactivity, the longer that our adversaries are able to establish their own norms."

Innovation

Too much money, (trillions of dollars) is being spent securing systems built on foundations that are inherently insecure. In an industry that has had a rate of change unprecedented in human history we should not be content to think that radical change is no longer possible. New tools, new products, new systems with transformational security paradigms should be investigated. Quantum computing threatens to make current encryption algorithms obsolete. What other technologies, software or hardware, might possibly tip the advantage back towards cyber defense?

Counter Arguments:

There are a variety of arguments made to suggest the perceived Chinese threat is exaggerated.

Some argue that the U.S. in fact has an overwhelming cyber superiority. In a 2021 study of the major cyber powers by the International Institute for Strategic Studies only the United States was ranked as Tier 1. (15) The study found that, "It is the only country with a heavy global footprint in both civil and military uses of cyberspace, although it now perceives itself as seriously threatened by China and Russia in that domain." The IISS further concluded that, "the US capability for offensive cyber operations is probably more developed than that of any other country."

Others suggest that China's military cyber capacity does not live up to its doctrinal aspirations. Jon Lindsay of the University of Toronto suggests that China demonstrates little skill or subtlety in their cyber operations. That the rigidly hierarchy of the Chinese military hinders their capabilities as does a lack of wartime experience. They, in fact, "face underappreciated organizational challenges, including information overload and bureaucratic compartmentalization, which hinder the weaponization of cyberspace or absorption of stolen intellectual property." (16)

Internal structural and political issues may also undermine its ability to capitalize on cyber gains. Insufficient arable land, a rapidly aging society, heavy reliance on energy imports, and stifling ideological and state-centered controls across society (17)

The idea that China may be able shift global norms toward an acceptance of its authoritarian model is also called into question. Foreign Policy magazine suggests that Beijing has little interest in exporting its governance system. That, "even if Beijing were to attempt to export its development approach to other states, the actual attractiveness of that approach would prove to be highly limited. The features undergirding China's developmental success are not replicable for most (if any) countries." (17)

They go on to claim that China's internal structural and political issues may also undermine its ability to capitalize on cyber gains. China's aging population, extensive corruption, very large levels of income inequality, inadequate social safety net, and the fact that free information flows are required to drive global innovation make its authoritarian model unsustainable. (17)

While the perceived U.S. advantage in cyber capabilities is likely accurate, focusing on this as an example of the exaggerated Chinese threat misses the difference in geopolitical endgames between the two countries. China exhibits a much greater willingness to engage in attacks and exploit weaknesses. Similarly puzzling is the suggestion that Chinese cyber operators lack skill in light of the many highly successful campaigns for which they have received attribution.

Arguments about internal issues are more convincing. The one child policy has resulted in a rapidly aging population, there are concerns the large collective debt of Chinese corporations will damage the economy, and technological innovation has historically flourished best in open societies. The question of Chinese weaknesses and to what degree they might limit their global aspirations is worth considering.

Still, Supposing that China is not a truly existential threat it still remains the most credible and capable threat actor with the most disruptive goals.

Conclusion

Information security has struggled to keep pace with the exponential growth of computing in nearly every sector of society. The lack of security has led to a feeding frenzy among bad actors. cyberattacks cost trillions of dollars a year worldwide and result in the breach of sensitive public, corporate and government information. It is a crisis affecting national security.

Among these threat actors, nation states possess the greatest potential for harm. They can employ considerable resources and have malign goals at a geopolitical level. Espionage, cybercrime, influence campaigns, surveillance, censorship, and direct cyberattack are all part of their digital toolbox.

Chief among these threats is China. It has the largest economy and therefore the greatest resources to develop cyber capabilities. In particular, it employs sophisticated espionage abilities to steal intellectual property in a effort to gain technological dominance. It perceives this as key component in a pathway to supplanting the U.S. as the predominant world power. Given the nature of its authoritarian regime and its willingness to censor and suppress both its own people and and foreign nationals this is a deeply troubling objective. For its disruptive goals and significant ability to pursue them China will be the biggest cyber threat actor of the next 5 years.

References

1. Kolokotronis, N., & Shiaeles, S. (2021). Cyber-Security Threats, Actors, and Dynamic Mitigation. *Milton: Taylor & Francis Group.*

2. Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine.* https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

3. Office of the Director of National Intelligence. (2022). Annual Threat Assessment of the U.S. Intelligence Community. *Office of the Director of National Intelligence.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

4. Center for Strategic & International Studies. (2022). Significant Cyber Incidents Since 2006. *Center for Strategic & International Studies*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/220404_Significant_Cyber_Incidents.pdf?6baqc92oMg0w.0wCwZLP6OATs9MmMmLG

5. Cybersecurity & Infrastructure Agency. (2022). North Korea Cyber Threat Overview and Advisories. *Cybersecurity & Infrastructure Agency.* https://www.cisa.gov/uscert/northkorea

6. Nichols, M. (2019). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. *Reuters*. https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

7. Fortinet. (2022). What is WannaCry Ransomware Attack? *Fortinet*. https://www.fortinet.com/resources/cyberglossary/wannacry-ransomeware-attack

8. Libicki, M. (2018). Could the Issue of DPRK Hacking Benefit from Benign Neglect? *Georgetown Journal of International Affairs, 19*(3), 83.

9. Cybersecurity & Infrastructure Agency. (2022). Iran Cyber Threat Overview and Advisories. *Cybersecurity & Infrastructure Agency.* https://www.cisa.gov/uscert/iran

10. Cybersecurity & Infrastructure Agency. (2022). Russia Cyber Threat Overview and Advisories *Cybersecurity & Infrastructure Agency.* https://www.cisa.gov/uscert/russia

11. Cybersecurity & Infrastructure Agency. (2022). China Cyber Threat Overview and Advisories *Cybersecurity & Infrastructure Agency.* https://www.cisa.gov/uscert/china

12. Panda, J. (2022). Shifting China-NATO Relations: From Selective Cooperation to Strategic Rivalry? *The Jamestown Foundation*. https://jamestown.org/program/shifting-china-nato-relations-from-selective-cooperation-to-strategic-rivalry/

13. Fischerkeller, M. (2020). Opportunity Seldom Knocks Twice: Influencing China's Trajectory via Defend Forward and Persistent Engagement in Cyberspace. *Asia Policy, 27*(4), 65-89.

14. U.S. Cyber Command. (2022). Achieve and Maintain Cyberspace Superiority. *U.S. Cyber Command*. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

15. The International Institute for Strategic Studies. (2021) CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment. *The International Institute for Strategic Studies*. https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf?la=en&hash=832036F094A4C489C313AC617643369E07FAE9F8

16. Lindsay, J. (2015). Inflated Cybersecurity Threat Escalates US-China Mistrust. *New Perspectives Quarterly, 32*(3), 17-21.

17. Swaine, M. (2021). China Doesn't Pose an Existential Threat for America. *Foreign Policy.* https://foreignpolicy.com/2021/04/21/china-existential-threat-america/