The Inevitable Battleground for Competing Powers: Cyberwarfare

https://www.e-ir.info/2020/10/05/the-inevitable-battleground-for-competing-powers-cyberwarfare/

MOHAMMED SEID AHMED AND MAKAM KHAN DAIM, OCT 5 2020

The internet has been an integral part of our lives since its commercialization in the mid-1990s. It has also become critical for our day-to-day activities, and it is impossible to think what our lives would be without it. Banks can perform transactions within a few minutes across the world, people can make payments from their smartphones, students can attend classes through their computer windows, one can pay your taxes, buy cars, sell goods, etc., thanks to the internet. As many countries are adopting digitalization in their development agenda, larger populations are being introduced to cyberspace. According to recent data, nearly 4.57 billion people are active internet users as of July 2020, which amounts to 59 per cent of the entire global population (Tsakanyan, 2017, p.339). China, India, and the United States are the top three countries with the number of internet users, respectively (Tsakanyan, 2017, p.339).

The opportunities that cyberspace provides for people around the world are enormous, but it has also given a platform for states and non-state actors to engage action from the likes of violating individual rights to undermining other nation-state's interests and sovereignty. The increasing connectedness of technological devices and reliance on cyberspace has also increased the vulnerability of people and governments to cyberattacks. The threat to cyberspace has not been more evident than today. State-sponsored hacking, theft of intellectual property rights, widespread misinformation, easy access to personal information and data of millions of people, and the increasing presence of non-state actors with their ability to effectively utilize cyberspace to promote their agenda, are all endangering the lives of many. Before this investigation goes any further, however, the question "what is cybersecurity?" must first be asked. Is cyberspace the next battleground for competing powers to wage unconventional war?

International Relations scholars, mainly in the field of security and strategic studies, have been studying the impact of technology on both national and international security. Their study focuses on power, sovereignty, global governance, and securitization (Maurer and Ebert, 2017). However, scholars and experts often conflate cybersecurity with information security. According to Craigen et al (2014, p.14), "cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Despite the lack of consensus among scholars on the definitions of cybersecurity, the broad definitions of the concepts include the different types of cyber threats. Namely, cyberwarfare, cyberconflict, cyberterrorism, cybercrime, and cyber espionage (Małgorzata, 2017). Cyber-attacks in any form present a threat to national and international security.

It is impossible to understand or discuss cyber threats without defining the term cyberspace beforehand. The most cited definition of cyberspace is the one that is given by the United States Department of Defense, which states that cyberspace is: 'a global domain within the information environment consisting of the independent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers' (Malgorzata, 2017). Cyberspace has created opportunities for millions of people around the world in various ways. It has also created opportunities for state and non-state actors to exploit the platform to advance their goals in a cost-effective way. In today's climate, a traditional military confrontation is no longer necessary, as nation-states can utilize cyberspace to undermine their rivals with low cost to human lives and a nation's economy. One factor that makes these threats more challenging for the future

is that it is often not easy to precisely determine the responsible party. One can stay anonymous while performing cyberattacks using a random uninformed user (Malgorzata, 2017). There are various types of cyberattacks – ranging from espionage to cyberwarfare. In today's environment, cybercrime, cyber terrorism, cyber espionage, and hacking are the primary modes of cyberattacks.

Cyberattacks and Its Different Forms

In 2016, the United States Intelligence community confirmed that a state-actor, Russia, allegedly interfered in the election process in order to discredit candidate Hilary Clinton and favor Donald Trump in the presidential election (Vesoulis, Abby, and Simon, 2018). This is a typical example of how state-actors hold the potential to undermine other nations, influencing the outcome of an electoral and democratic process by utilizing cyberspace effectively. Thus, cyber-attacks could threaten the very essence of representative democracy, where the voice of the people does not matter anymore. Interested groups or candidates could conspire with state or non-state actors in order to win power, threatening democratic institutions through the potential of democratic backsliding.

The other intent for state-actors to engage in cyberattacks is for purposes relating to espionage. Cyber Espionage is defined as the unauthorized access to sensitive, confidential, or classified information (Vesoulis, Abby, and Simon, 2018). China has been the major actor for allegedly stealing intellectual property rights, trade secrets, and military documents from its main rival, the United States, according to the recent US Department of Defense (DOD) report to Congress (USDOD, 2019, p.39). Most recently, Russia was again accused of stealing laboratory data on COVID-19 vaccinations by its Western counterparts (Barnes, 2020). Thus, state-actors can directly or indirectly engage in cyber-attacks to advance their national interest.

There is another type of cyber operation called "cyber coercion," as identified by the Rand Corporation research paper entitled, "Understanding and Countering Cyber Coercion" (Hodgson et al, 2019). The research focuses on – Iran, Russia, China, and North Korea that are identified by the United States government as a threat to national security (Hodgson et al, 2019). Although the report found that it amounts to a smaller portion of the overall cyber operations, there are some instances that these nation-states engage in coercion to protect their national interest. China's cyber operation primarily focuses on espionage, however there were times that China has utilized cyber operations for coercion purposes. For instance, in 2016 when South Korea allowed the US to deploy the THAAD (Terminal High Altitude) missile defence system, China was angered with its neighbours' decision (Hodgson et al, 2019). The report further discovered that there was an increase in cyber-attacks that has served as a statement from China to demonstrate its displeasure with the THAAD deployments in close proximity to its territory.

All the above-mentioned threats have significant implications for national and international security, but two types of cyber operations could eventually threaten even the existence of humanity. Cyberwarfare and cyberterrorism are not given serious thought by policymakers and governments because states are too consumed with the common type of cyberattacks, namely espionage and hacking. As our lives are intertwined even more so with the advancement of technology, there is a desperate need to address cybersecurity to protect people from these threats. Perhaps, the lack of major attacks that could be attributed to cyber warfare and terrorism could be the reason. The globalized world has interconnected our interests, and we are bound together without even being aware of it. For instance, a cyberattack on any major economy, like China, would disrupt global economic activity and have a serious implication for the world. In the age of social media and increased network connectedness, cyber operations could easily exploit the opportunity to create a civil disturbance with the spread of misinformation. If transnational non-state actors manage to get control of any sensitive material in the cyber domain, the repercussions could be costly. With today's technology, such as 5G networks and AI (Artificial Intelligence), the opportunity for states and non-state actors alike to cause great damage to humanity is increasing.

The use of cyber operations to wage war is not something new. It has started since the development of computers and technological advancement. There was limited use of cyberspace in armed conflict during the first US-Iraq war that was dubbed 'Operation Desert Storm', NATO's intervention in Kosovo in 1999, and the second US invasion of Iraq in 2003 (Malgorzata, 2017, p.10). The initial use was limited because these Western nations sought to hide their technological advancement, and in the case of the Iraq invasion, the US did not want to use its full capability mainly

for legal reasons (Malgorzata, 2017, p.10). There are some other instances that states had engaged in cyber-attacks to destroy critical infrastructures of their rivals. Given the current technological advancement and increasing animosity between regional and international powers, it is likely to continue in the foreseeable future.

How Are Countries Addressing Cybersecurity?

Different countries are taking risk management by their own account, but there is a lack of international coalition to address this existential threat. For instance, in 2014, President Xi Jinping of China declared that there is: "No national security without cybersecurity" (Tsakanyan, 2017, p344-45). Among the measures China is taking to strengthen cybersecurity, to limit foreign investment in critical infrastructures like Information Communication Technology (ICT) is significant. Global powers are engaging in a tit for tat measure, accusing the other of espionage and hacking.

On the state-level, China's President Xi has called for cyber-sovereignty on multiple occasions in his vision of cybersecurity and governance (Barnes, 2020). In other words, the government should be responsible for controlling cyberspace within one country's territory and any company, foreign or domestic, must comply with the rule and pass on pertinent data to the government. President Xi's approach is very much in line with authoritarian governments around the world. More importantly, it will be the end of personal freedom and rights. Companies are already complying with Xi's approach due to the vast Chinese market and its economic clout. This does not mean other companies and so-called democratic governments are not spying on their citizens or accessing private information. However, in democratic countries, if citizens become aware of the violation of their privacy, they can pursue legal actions against the government or companies. However, in non-democratic countries it is a way for authoritarian governments to suppress freedom and control their citizens' freedom of expression.

Nonetheless, as technology is advancing at a faster pace than human civilization, it is unlikely for nuclear-armed nations to wage conventional war against the other. Cyberwarfare presents a great opportunity for global powers, middle powers, and even for non-state actors to pursue destructive goals. It is insidious and subtle with a devastating consequence for the world.

Indeed, Cyber-attacks could turn into complete cyberwarfare if nations are not working together to address this pressing issue in a timely manner. The United Nations in December 2018, passed resolution 73/266 to establish a Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UNODA, 2019). The UN move was important and timely, but yet to come to fruition. It must bring global powers and initiate a rule that everyone should abide in and prevent nations from the proliferation of cyber-attacks for the benefit of humanity. Moreover, there is more to achieve if global powers work together to strengthen cybersecurity to protect critical infrastructure and military arsenals from falling into the hands of non-state actors. Nonetheless, between major powers, there is a consensus on the threat of climate change to human existence in which many countries are already working together to mitigate the effect. However, these nations tend to neglect other important issues like the threat of nuclear weapons and cyberwarfare. The competition between global powers and other state-actors to make cyberspace the next battleground will have a serious consequence for the rest of the world if not addressed collectively in a timely manner.

References

Barnes, J., (2020). 'Russia Is Trying To Steal Virus Vaccine Data, Western Nations Say.' [online] *Nytimes.com.* Available at: <https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html> [Accessed 17 September 2020].

Craigen, D., Daikun-Thibault, N., Purse, R., 2014. 'Defining Cybersecurity'. Technology Innovation Management Review.

Ebert, H., Maurer, T., 2017. International Relations and Cyber Security: Carnegie Contribution to Oxford Bibliographies. https://carnegieendowment.org/2017/01/11/international-relations-and-cyber-security-carnegie-

contribution-to-oxford-bibliographies-pub-67672 [Accessed 05/10/2020].

Hodgson, Q., et.al., 2019. 'Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace, Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace'. *RAND Corporation*. doi:10.7249/rr296.

Małgorzata, B., 2017. 'Cybersecurity as The Basic For State and Society Security in the XXI Venstury'. Safety & Defense 3(1), 8–13. doi:10.37105/sd.1.

Tsakanyan, V.T., 2017. 'The Role of Cybersecurity in World Politics'. Vestnik Rudn International Relations, 17(2), 339–348. doi:10.22363/2313-0660-2017-17-2-339-348.

UNODA, 2019. 'Group of Governmental Experts – UNODA', *United Nations Office for Disarmament Affairs*, https://www.un.org/disarmament/group-of-governmental-experts/, [Accessed 05/10/2020].

US DOD, 2019. 'Annual Report To Congress: Military and Security Developments Involving the People's Republic of China 2019', *United States of America Department of Defence*, https://www.hsdl.org/?abstract&did=824747 [Accessed 05/10/2020].

Vesoulis, A., Simon, A., 2018. 'Here's Who Found That Russia Meddled in the 2016 Election'. *Time*. https://time.com/5340060/donald-trump-vladimir-putin-summit-russia-meddling/ [Accessed 05/10/2020].

About the author:

Mohammed Seid Ahmed M.Phil International Relations, Zhejiang University, currently based in California, USA.

Makam Khan Daim is studying Security, Intelligence and Strategic Studies in a consortium degree program at University of Glasgow, (UK), DCU (Ireland), OTH (Germany), and Charles University, Prague. Mr. Daim studied M.Phil. International Relations at Zhejiang University, China and BS (Hons) Politics and International Relations, and received a Gold Medal in the mentioned subject, at the International Islamic University, Islamabad from the President of Pakistan.