The Reversion of Cyberspace to the World of Classical Realism

Author Jun Osawa

By Jun Osawa

The post-Cold War era has come to an end, and classical realism has returned to international politics. The world of classical realism is a world in which the state is the main actor, and the existential security of the state is the primary concern. Cyberspace is no exception to this recursive phenomenon in international politics.

Over the last 10 years, some states have been using cyberspace as a place to achieve strategic goals and express their intentions, beginning with the use of cyberattacks against the Baltic States in pursuit of national interests. In cyberspace, where attackers can easily hide their identities, the state-to-state conflict in a realist world reemerges with intensity.

State-Sponsored Cyberattacks on the Rise

On April 27, 2007, Estonia, one of the three Baltic States, suffered a massive distributed-denial-of-services (DDoS) attack on its government, parliament, media, and banks. This cyberattack was executed through a botnet consisting of tens of thousands of computers around the world whose control had been taken away without their owners' knowledge. The following month, a second wave of an even greater DDoS attack hit Estonia, paralyzing online banking and ATMs and otherwise thrusting people's daily lives into utter chaos.

Triggering the attack was an international dispute between Estonia and its neighbor Russia over the removal of a statue of a Red Army soldier erected during the Soviet occupation. With Russian support, Estonia's ethnic Russian citizens opposed its removal, and the Estonia-Russia relationship deteriorated dramatically. Later, it was discovered that the master computer that controlled the botnet used in the cyberattack had been located in Russia and operated using a Cyrillic keyboard. Thus, it is believed that the Russian government or a group closely connected with it was behind the cyberattack.

Among other former Soviet Union republics in disputes, like Estonia, with Russia, Lithuania in June 2008, Georgia in August 2008, and Kyrgyzstan in January 2009 each suffered a "denial of functional service" attack. In Georgia's case, the cyberattack coincided with the Russian invasion of South Ossetia, where ethnic conflict had reared its head. The threat of a "hybrid conflict" combining a kinetic attack and a cyberattack had become reality.

As for other neighbors of Russia, in December 2012, Ukraine, which had been embroiled in armed conflict with Russia, became the stage for the world's first state-sponsored cyberattack on critical infrastructure. On Dec. 23, the power transmission system of Prykarpattyaoblenergo, which supplies electricity to western Ukraine, suffered a cyberattack in which its control system was hijacked and several substations were forcibly shut down, resulting in the loss of power for 220,000 households for several hours. A similar attack occurred in December 2016 in Kyiv, Ukraine's capital. The Ukrainian government has blamed Russia for the series of attacks.

In June 2016, also against Ukraine, there was a massive cyberattack using the malware Not-Petya. Not-Petya is highly toxic, making all the data on the hard disks of the computers that it infects unusable by encrypting them. Since the malware used MeDoc, an accounting software used in Ukraine as the initial infection route, and focused its harm on the government, transport systems, critical infrastructure and the like in Ukraine, it was seen originally as a geographically limited cyberattack focused on Ukraine. However, because of its highly infectious nature, global companies with branches in Ukraine were hit one after another by the malware, including some of the most prominent businesses in the world such as Mærsk (Denmark, shipping), Mondelez (United States, food products), FedEx (US, air freight), and WPP (United Kingdom, advertising agency).

Immediately after the first cyberattack, the Ukrainian government accused the Russian government of being the perpetrator. Western corporations were also victims, and the Five Eyes — the US, the UK, Canada, Australia, and New Zealand — after painstaking research, confirmed that the Not-Petya cyberattacks had been conducted by the Russian government and issued a joint statement on Feb. 15, 2018 condemning Russia.

In the Middle East, an attack came to light in 2010 that was aimed at Iranian uranium enrichment facilities using the malware Stuxnet. This malware was used in a function-destroying attack to paralyze the control system for the centrifuges essential to producing enriched uranium by targeting the programmable logic controllers (PLC) manufactured by Siemens. It has been revealed that there was a retaliatory attack in 2013 by Iran against the US, identified as the source of the Stuxnet attack by the media, on a dam in the state of New York. Iran is also believed to have been involved in the August 2012 attacks targeting Saudi Arabia and Qatar's energy companies and the November 2016 attacks on Saudi government institutions and companies.

East Asia is also the stage for a heated cyberwar. North Korea has launched continuous function-impeding/function-destroying cyberattacks on South Korea. In July 2009, there was a function-impeding cyberattack on government institutions, financial firms, and media companies. In March 2013, there was a function-destroying cyberattack that erased data from infected computers in media companies and financial institutions. In 2014, there was a cyberattack on Korea Hydro and Nuclear Power Corporation (KHNP). The South Korean government published a report on this series of attacks that points to North Korea as the culprit.

The cyberattack group that North Korea seems to be the hand behind appears to be very highly skilled. Beginning with the 2014 attack on Sony Pictures in the US, it has been actively conducting attacks for acquisition of foreign currency since 2016 on central banks and other financial institutions of Bangladesh and other countries, raising widespread concerns.

Shockwaves from Cyber-pandemic WannaCry

It has been some time since we began seeing news on such cyberattacks daily. But in May 2017, there was a cyberattack that astonished experts — the emergence of WannaCry, a new type of ransomware with an explosive infectious capacity. It was a typical malware that encrypted files in an infected computer and issued a demand to the victim to pay around US$300 in bitcoins to unlock the files, but the process of spreading the infection was of an unprecedented seriousness. On infection, this malware immediately activates an infecting module that spreads the malware to computers in the same network and beyond. WannaCry accordingly infected more than 300,000 computers in more than 150 countries worldwide in less than 10 days since it was detected, creating a cyber-pandemic.

In the UK, WannaCry had a serious impact on the lives of the people there, as the National Health Service (NHS) network was infected, making it impossible to access patients' medical records, halting the acceptance of ambulances, and suspending surgery operations. Elsewhere, the French auto manufacturer Renault, the German railway company Deutsche Bahn, the Spanish telecommunication giant Telefonica, the Brazilian oil company Petrobras, and others were found to be infected. The infection even spread to government institutions believed to be equipped with tight security such as the Russian Ministry of Internal Affairs and China's Ministry of Public Security.

In Japan, Hitachi and its group companies were infected through its global network, causing paralysis in its email system. Honda's Sayama Plant shut down temporarily due to the infection. McDonald's Japan was infected by an altered version of WannaCry with the result that payments using points and electronic money had to be suspended.

It was later revealed through forensic investigation by cybersecurity firms that Lazarus, a cyberattack group connected to North Korea, was involved in its creation. In the UK, the government conducted an analysis led by the National Cyber Security Centre (NCSC), and the national security authorities determined that North Korean hackers had been involved in the attack.

Lazarus is believed to be the perpetrator of the 2014 cyberattack on Sony Pictures Entertainment and the illegal transfer through the SWIFT settlement system that defrauded the Bangladesh Central Bank of $81 million. It is considered a virtual arm of the North Korean government.

WannaCry was able to cause such widespread infection and damage that it was deemed to be the world's first cyber-pandemic because it spread infection by exploiting the vulnerability of the Microsoft Server Message Block (SMB) file-sharing protocol of the Windows operating system. This vulnerability was first published by Microsoft in September 2016 and the MS17-010 security patch for it was released in March 2017. However, PCs and servers that had not applied the patch remained worldwide, leaving them critically vulnerable to certain infection when attacked by WannaCry.

The infiltration tools used to exploit this vulnerability are entitled EternalBlue, which executes any given order to exploit a vulnerability, and DoublePulsar, the backdoor point of entry that it creates. Believed to be developed originally by the US National Security Agency (NSA) to penetrate foreign networks, North Korea was able to use them because a Russian hacking group named Shadow Brokers had leaked the tools on the Internet in April 2017. The fact that a cyberattack incorporating these powerful infiltration tools was conducted less than a month after they had been dumped sent a shockwave through the cybersecurity community. Even more serious was the fact that government-level, cutting-edge cyberattack tools had been used indiscriminately against computers worldwide possessed not only by governments but also by private-sector firms.

Escalating Cyberattacks on Japan

In addition to cyberattacks aimed at impeding functions and control systems, targeted attacks involving governments with the objective of stealing confidential information from specific organizations and individuals are also on the rise. In Japan, a large-scale targeted attack (advanced persistent threat: APT) aimed at stealing information from the House of Representatives, government institutions, and the defense industry came to light in 2011. Similar attacks with the objective of stealing information are believed to have taken place intermittently since around 2005. In May 2015, a targeted cyberattack aimed at the personal information that the Japan Pension Service (JPS) possesses took place.

The Emdivi malware was used in the cyberattack on the JPS. According to the report by the National center of Incident readiness and Strategy for Cybersecurity (NISC), which investigated the cyberattack on the JPS, the first wave hit on May 8, 2015. Four more waves followed, infecting more than 30 computers and leaking personal information on 1.25 million individuals in all. Macnica Networks, which conducted a technical analysis of the malware, concluded that the creator of the malware was someone in China who worked between 9 a.m. and 5 p.m. from Monday to Friday. There is strong suspicion that China is involved. APT groups in China repeatedly conducting information-theft cyberattacks have been stepping up their attacks on Japan, particularly since 2016, according to analysts. The situation requires close monitoring from now on.

Information-Manipulating Cyberattacks as Threat to Democracy

Moreover, as a new phenomenon in the recent trend of cyberattacks, manipulative cyberattacks (information warfare) aimed at information manipulation within other states against the background of inter-state conflicts are taking place. During the 2016 presidential election in the US, it is believed that Russian cyberattack groups APT28 (FancyBear) and APT29 (CozyBear) conducted information-theft cyberattacks and distributed internal information taken from the Democratic Party through Wikileaks. In addition, distributing "fake news", sowing confusion through cyberattacks through proxies, and deliberately releasing stolen confidential information are said to have had a significant impact on the ultimate outcome of the presidential election. Similar information-manipulation cyberattacks took place in 2017 in the French presidential election and the German general election, with each country struggling to respond.

Deterring State-Sponsored Cyberattacks

As we have seen, cyberspace is being used as a stage on which intelligence activities, impeding functions, destructive acts, and information manipulation are being used to achieve national strategy objectives and express intentions. Moreover, highly infective and destructive malware are emerging in succession, increasing the risk of serious cyber-pandemics on a global scale.

The US against China, the US and Europe against Russia, the US against North Korea: these states are already attacking each other through cyber-intelligence, functional impediments, and destructive attacks. At this moment, matters have remained in a "gray zone" that does not reach a state of "war". However, highly infective and destructive malware are emerging in succession, increasing the risk of serious cyber-pandemics on a global scale.

In Japan, cyber-theft by Chinese actors is conspicuous, but a large-scale cyberattack aimed at critical infrastructure has yet to occur. However, concern is growing as changes in the international environment or the emergence of a global cyber-pandemic could have a massive impact on people's lives in Japan.

The US appears to recognize that ensuring cybersecurity, protecting critical infrastructure, and other forms of passive defense are insufficient, and is infiltrating and continuously monitoring activities in other countries and accumulating vast amounts of electronic information from the Internet, and conducting post-event analysis and follow-up using big data analysis.

Indeed, the US cybersecurity strategy published in 2015 consists of both enhancing "cyber deterrence by denial" by improving its cyber robustness and resilience and enhancing "cyber deterrence by punishment" consisting of a variety of policy tools including cyber-counterattack. It places deterring state-related cyberattacks at the center of the national cyber security.

The national response to cyberattacks has focused on passive cyber-defense such as securing cyber-security and protection of critical infrastructure. A more proactive cyber-defense by such means as continuous monitoring of attacking groups and responses to attacks using big data analysis is now in order. JS

Jun Osawa joined the Institute for International Policy Studies (IIPS) in 1995 and has been senior research fellow since 2009. He has also concurrently served as senior fellow of the National Security Secretariat (NSS) in the Cabinet Secretariat. He has served in several government and academic positions, such as at the NSS, Japanese Ministry of Foreign Affairs (MOFA), the National Graduate Institute for Policy Studies (GRIPS) in Tokyo, and the Brookings Institution in the United States.