


BLUE PEACE BULLETIN

VOL 10/NOVEMBER 2019

WATER AND VIOLENCE: CYBER ATTACKS AND CYBER WARFARE

Strategic Foresight Group



The Global High Level Panel on Water and Peace called for protection of water resources and infrastructure from violent conflicts and terrorist acts. In this volume, we examine the emerging threat of cyber attacks on critical infrastructure.

CYBER ATTACKS AND CYBER WARFARE

Introduction

Water infrastructure across the globe is being digitised and automated much like any other critical infrastructure. While this phenomenon is quite common in western nations, other parts of the world are also entering into this process of digitization of water systems. Most water utilities in several parts of Africa for example are getting digitalised whether it is in the realm of water treatment works or data collection and analysis.

Computer networks and systems perform numerous critical functions such as raising dam gates, operating pumps and purifying water. Therefore, it is also vulnerable to cyber threats and attacks like any other infrastructure system. It is predicted that cyber-attacks against critical infrastructure of a nation including water infrastructure could become a means of war in the future. There is also the issue of avoiding a 'cascading effect' due to the interconnectedness of water with energy and public health systems.

Attacks against water infrastructure could be by both state and non-state actors. Cybersecurity risks could be seen in different forms such as cyber-crime, espionage, 'hacktivism', terrorism or warfare. Globally, cyber security risks are on the rise in general. Globally, cyber-crimes happen every sixty seconds, costing more than \$600 billion USD in 2018 alone. About 30 Phishing attacks are said to happen every minute while ransom-ware victimizes 1.5 companies per minute. While cyber-crimes mostly create an impact in the economic sphere, there are also attacks that specifically target real world infrastructure including water. This form of attack on critical infrastructure which would affect lives of people is

also on the rise. Furthermore, it is predicted that weaponization by state or armed non state actors/terror groups to destroy critical infrastructure could be the next major international crisis that the world would witness. There have been instances of cyber-attacks and predicted risks/threats against water infrastructure in the past. Some of the examples are as follows:



2009-2010: A computer worm, named Stuxnet was created by the U.S with assistance from Israel to infect the Iranian nuclear programme. The worm was created to make the centrifuges of the nuclear plant to turn more rapidly than appropriate. Thereby causing Iran's nuclear programmes a set back by 'several years.' Stuxnet is said to be the 'first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.'

2013: Israeli officials reported a failed attempt by the Syrian Army to compromise water supply to the city of Haifa in Israel.

2013: The U.S. Army database that holds sensitive information about vulnerabilities in 79,000 dams throughout the U.S. was hacked. The database tracks information regarding the number of estimated deaths that could occur if a specific dam failed.

2013: Iranian 'hactivists' were able to identify and exploit vulnerabilities of the Bowman Dam in the U.S through a process called "Google Dorking". However, the attack was thwarted due to the fact that the gate was manually isconnected for maintenance thereby preventing serious harm.

2014: The FBI confirmed that operatives in China, Iran and Russia were doing a mapping operation, looking for cyber security weaknesses in the country's (USA) water and electric infrastructure.

2015: In December 2015, Russia was able to hack and shut down Ukraine's power grid. After the attacks, the U.S. government issued warnings to not just American power companies but also to water suppliers that same such methods of attack could be used against them.

2015: The Department of Homeland Security (DHS) of the US released a report that showed that water grid was vulnerable to attacks by hackers. It said that the water utilities were most likely to have "an advanced persistent threat".

2016: American public utility company Lansing Board of Water & Light (BWL) announced that the company has become a victim of a ransomware attack where



cyber-criminals locked BWL out of its own systems and demanded the equivalent of \$25,000 in Bitcoin to recover access. Replacing the infected computers and software cost \$10 million, and full remediation costs were approximately \$2.4 million. It is unclear whether the ransom was paid.

2018: The FBI and Department of Homeland Security issued a joint technical alert to warn of Russian cyber-attacks against US critical infrastructure. Targets included energy, nuclear, water, aviation, and manufacturing facilities.

2018: Cyber security researchers of Ben-Gurion University of the Negev (BGU), Israel, warned of potential distributed attack through the use of a botnet against urban water services of smart irrigation systems that water simultaneously. A botnet is a large network of computers or devices controlled by a command and control server of a malicious person or entity.

Norms Applicable

When the issue of cyber risks and attacks are examined, it is often done through prism of national or international security. Therefore some of the norms mentioned below are said to be applicable in such situations. However, it is still a widely debated topic with no concrete consonance even among scholars as to what norms would be applicable in the contexts of cyber security. The norms are as follows:

State Sovereignty

A cyber-attack could be considered as violation of Article 2(4) of the UN charter which states “All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.” If there is an attack on water infrastructure of a nation, it

could be considered a violation of state sovereignty guaranteed under the UN charter. However, in situations of cyber-attacks, the difficulty that arises is of attribution. Furthermore, this provision is only applicable to acts of States and not non-state actors. Right to Self Defence If through acts of cyber-attack a State is said to have violated sovereignty of another state in contravention to the UN charter, then the right to self-defence given under Article 51 of the UN charter can be invoked. This is seen in the 2011 International Strategy for Cyber Space of U.S which states “When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military partners.”

International Humanitarian Law (IHL)

IHL will only be applicable if cyber-attack occurs during or triggers an armed conflict. However, it must be noted that there are no specific provisions in the Geneva Conventions and it's Protocol that address the issue of cyber warfare or cyber-attack. Scholars have agreed that the general provisions applicable to conventional attacks can be applicable in the cases of cyber-attacks with the caveat that the attacks should have been carried out in the course of an armed conflict or have triggered an armed conflict. While IHL applies to both state and armed non state actors unlike the UN charter provisions mentioned above. Issues with regards to its applicability still arise. It is difficult to determine whether a cyber-attack could constitute the ‘use of force’ or an ‘armed attack’ in order for IHL to apply. Attribution of an attack to a State or an armed group could also be a problem when determining the applicability of IHL.

Non-intervention

The principle of non-intervention in a nation's air, maritime, or territorial space or in the economic sphere is broader than the principle of sovereignty. The principle has been reiterated through decisions of the ICJ, the UN General Assembly Declaration on Friendly Relations, the OAS Convention on the Rights and Duties of States in the Event of Civil Strife, and other authoritative sources. The ICJ has referred to some of this conduct as 'less grave forms' of force that violate the principle of non-intervention while not triggering rights of a victim under Article 51 of the UN charter. It is said that the principle would help to cover most situations which cannot be addressed through the principle of sovereignty or IHL.

Regional Legal and Cooperative Measures

It must be noted that in general, critical infrastructures across the globe have largely been secured against accidents or any kind of physical threat. However, there is not sufficient effort undertaken on understanding and taking concrete measures on ensuring that cyber security threats can be prevented or countered. Domestic measures do exist such as the UK Centre for the Protection of National Infrastructure (CPNI) which has been charged with protecting the UK's CNI from both physical and electronic attacks. Some noteworthy regional measures also do exist. The 2016

European Directive on Security of Systems and Individual Networks (NIS directive) lead to the creation of 'cooperation group' between all members states to promote cooperation and exchange of information relating to cyber security. In this context, European Union's 2013 cyber security strategy is also noteworthy as it pledges to identify vulnerabilities in European Union's critical infrastructure. The African Union also adopted a convention in 2014 on Cyber Security (Malabo Convention). However, it does not specifically address protection of critical infrastructure, although measures taken under the convention could help towards its protection.

As discussed in the Blue Peace Bulletin of Strategic Foresight Group of June 2019, "an international or regional framework and platform which specifically deal with the issue of cyber-attacks against water infrastructure is largely lacking. Strong international and regional cooperation is pertinent to effectively combat cyber-crimes due to its non-physical cross border nature. Nevertheless, an international or regional framework and platform which specifically deal with the issue of cyber-attacks against water infrastructure is largely lacking which makes it extremely difficult for nations to collaborate and share intelligence."



RECOMMENDATIONS

Encourage Cyber Pacts

Cooperation between nations in the realm of cyber security is an important measure to prevent attacks against critical infrastructure such as water. In this regard, the Paris Call of 2018 is noteworthy. It is a non-binding agreement launched by the President of France, Emmanuel Macron and supported by '67 States, 139 international and civil society organizations, and 358 entities of the private sector'. It states "We condemn malicious cyber activities in peacetime, notably the ones threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure and welcome calls for their improved protection." However, the instrument saw the absence of support from some of the world's active players in the cyber space including United States, Australia, Russia, China, Iran, North Korea and Israel. The hope is that in the future, these nations would also come on-board to signing cooperation pacts such as the Paris Call which could later pave the way for a more binding cooperative arrangement.

Exploring the Applicability of Existing Norms


As mentioned previously, the development of specific laws and norms applicable to cyber-attacks on water infrastructure is in a nascent stage. However, what the international community is also attempting to do is to interpret already existing laws including in UN charter and Geneva Conventions to instances of cyber-attacks. The Tallinn Manual of 2017 "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" commissioned by NATO Cooperative Cyber Defence Centre of Excellence is one such example. It has been authored by 19 international law experts. The manual aims to ensure that the vacuum created by the lack of a specific international or regional instrument is addressed through the interpretation of already

existing laws. This is an important endeavor to ensure that States have rights and obligations under international law when it comes to cyber threats or attacks.

Legal Frameworks

It would be ideal to have comprehensive international and regional legal frameworks that would specifically address the issue of protection of water resources from cyber-attacks which encourage information sharing among states to help mitigate consequences of cyber-incidents against water infrastructures. Although, one of the reasons for this to not come about is also due to the fact that it could amount to the regulation of internet which is opposed by many. However, instances of treaties that are considered dual uses such as the Chemical Weapons Convention (CWC) which prohibits the use or possession of chemical weapons, while also promoting legitimate uses of chemicals for civilian purposes can serve as a good starting point for legal instruments in the arena of cyber-attacks against water infrastructure. Furthermore, the issue of attacks or threats by non-state actors can also be addressed effectively.





Compensation/ Reparations

Some scholars are of the view that when it comes to cyber-attacks, the estimation of damages can be done in a more accurate manner than in the case of traditional warfare. In such a situation, reparations for a state that has been a victim of cyber-attack on water infrastructure can be demanded. In the case of purely financial damages, States can ask for compensation or other measures against another State akin to those remedies awarded for trade related damages under the rules of the WTO. However, the difficulty with demanding compensation or reparations is that it is contingent upon being able to attribute the incident to another nation or entity. Evidence regarding the same can be very difficult to come by.

Anticipating Future Threats

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) organises an annual exercise which is the 'largest international live-fire cyber defence exercise in the world' called Locked Shields that enables cyber security experts to enhance their skills in defending national systems and critical infrastructure under real-time cyber-attacks. "The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects." The scenario for 2019 exercise was of a fictional country, Berylia, experiencing a deteriorating security situation, with coordinated cyber-attacks against causing severe disruptions in the "power generation and distribution, 4G communication systems, maritime surveillance, water purification plant and other critical infrastructure components." Interestingly real network infrastructure provided by companies like Siemens and water-treatment systems from South Korea was involved in the simulation exercise. Such exercises should be further encouraged in all parts of the world in order to make critical water infrastructure more resilient to future cyber threats.

REFERENCES

Amnegor Jacob, «Cyber Security of / for Water Utilities in Africa», International Water Association(IWA) 07 June 2019 <https://iwa-network.org/cyber-security-of-for-water-utilities-in-africa/>

Brett Walton, «Water Sector Prepares For Cyberattacks», Circle of Blue, 09 June 2016 <https://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/>

«Significant Cyber Incidents Since 2006» Center for Strategic and International Studies, August 2019 https://csis-prod.s3.amazonaws.com/s3fs-public/190813_Significant_Cyber_Events_List.pdf

Mary Ellen O'Connell & Louise Arimatsu «Cyber Security and International Law» Chatham House, 29 May 2012 <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf>

«Hacker Breached U.S. Army Database Containing Sensitive Information on Dams»Wired, May 2013 <https://www.wired.com/2013/05/hacker-breached-dam-database/>

«Cyber-Attack Against the Bowman Avenue Dam»Nationa-e, 04 August 2016 http://www.nation-e.com/blog/new_page_759

«U.S. to blame Iran for cyber attack on small NY dam» Reuters, 11 March 2016 <https://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WC2NH>

«As Water Utilities Move Online, Hackers Take Note»Governing, February 2017 <https://www.governing.com/columns/tech-talk/gov-water-utilities-cybersecurity-hackers.html>

Judith H. Germano «Cybersecurity Risk & Responsibility in the Water Sector» American Water Works Association,2019 <https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013>

«New cyberattacks against urban water services possible, warn researchers»PhysOrg, 09 August 2018 <https://phys.org/news/2018-08-cyberattacks-urban.html>

«UN Charter» Last Accessed 11 September 2019 <https://www.un.org/en/sections/un-charter/chapter-i/index.html>

«Cyber warfare and international humanitarian law: The ICRC's position», ICRC, June, 2013 <https://www.icrc.org/en/doc/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf>

«Talin Manual 2.0» CCDCOE, Last Accessed 11 September 2019 <https://ccdcoe.org/research/tallinn-manual/>

Jenna McLaughlin «How Europe's smallest nations are battling Russia's cyberattacks» Heinrich Boll Stiftung, 02 July 2019 <https://us.boell.org/2019/07/02/how-europes-smallest-nations-are-battling-russias-cyberattacks>

Nazli Choucri, Stuart Madnick, Priscilla Koepke«Institutions for Cyber Security: International Responses and Data Sharing Initiatives:Working Paper», Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, August 2016 <http://web.mit.edu/smadnick/www/wp/2016-10.pdf>

«Blue Peace Bulletin: Regional Water Protection Framework» StrategicForesight Group, June 2019 https://www.strategicforesight.com/publication_pdf/REGIONAL%20WATER%20PROTECTION%20FRAMEWORK.pdf

«National Cyber Security Strategies», European Union Agency for cyber Security, Last Accessed 11 September 2019 <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>

«Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms», Council on Foreign Relations, 23 February 2018, <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms>

«International cooperation on cybersecurity matters», UNODC, Last accessed 16 September 2019 <https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html>

Elena Chernenko«Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms», Council on Foreign Relations (CFR), February 2018 <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms>

Cat Zakrzewski «The Cybersecurity 202: The U.S. was notably absent from a global cybersecurity pact. But American companies signed on» , Washington Post , November 2018 <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/11/13/the-cybersecurity-202-the-u-s-was-notably-absent-from-a-global-cybersecurity-pact-but-american-companies-signed-on/5be9c0881b326b3929054751/>

«Paris Call for Trust and Security in Cyber Space» November 2018 https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Strategic Foresight Group is an international think tank based in Mumbai, India. Since its inception in 2002, it has worked with governments and national institutions of 60 countries in four continents. It is known for conceiving several pioneering policy concepts to help decision makers to respond to challenges of the future in three spheres: peace and security, water diplomacy, global paradigm shifts.

Its ideas have been discussed in the United Nations Security Council, United Nations Alliance of Civilizations, Indian Parliament, European Parliament, UK House of Commons, House of Lords, World Bank, World Economic Forum (Davos) and other important public institutions. The initiatives and analysis of the Strategic Foresight Group have been quoted in over 3000 newspaper articles and news media sources from almost 100 countries in all continents.

www.strategicforesight.com

Blue Peace Bulletins are produced by Strategic Foresight Group as a part of a programme co-financed by the Swiss Agency for Development and Cooperation (SDC). They do not in any manner represent the official position of the SDC or any other branch of the Government of Switzerland.