Karlsruhe Model United Nations

23 - 25th November 2018

Maria Krasnova
Florian Böhm

Security Council

Study Guide

Contents

Topic: Critical Infrastructure Protection in the context of cyber attacks

I. Introduction

Critical Infrastructure Protection (CIP) becomes more and more important with the digitisation of economy, politics and society. Critical infrastructure becomes more connected with the internet and therefore becomes more vulnerable. Besides conventional attacks by hostile forces and natural disasters, also via cyberattacks. Therefore plans by national agencies recently started to acknowledge this new threat and try to tackle it.

International cooperation is key to effectively protect against cyber attacks, sharing resources and knowledge can help to prevent such attacks and create better response systems in case an attack is successful.

So at this years UNSC at KAMUN 2018 we want to discuss this new threat to the critical infrastructure systems in the world.

II. Explanation of Terms

In this section we want to provide you with basic definitions for the upcoming discussion. We're gonna define the terms Critical Infrastructure, protection and cyber attacks in the context of critical infrastructure.

a. Critical Infrastructure

According to the European Commission:

"Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens."[1]

This definition is similar to the one provided by the U.S. Department of Homeland Security:

[1] ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

“Overall, there are 16 critical infrastructure sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The National Protection and Programs Directorate's Office of Infrastructure Protection (IP) leads the coordinated national effort to manage risks to the nation's critical infrastructure and enhance the security and resilience of America's physical and cyber infrastructure.”[2]

Based on these definitions it becomes clear that critical infrastructure is characterized as an infrastructure sector which is vital for the survival and persistence of modern society. Damage to these sectors would most likely destabilize society and threaten the security of the state.

To illustrate the importance of these sectors Homeland Security names 16 sectors which require special protection: The chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agricultural sector, government facilities sector, healthcare and public health sector, information technology sector, nuclear energy, materials and waste sector, transportation systems sector and water and wastewater systems sector.[3]

This classification however is not common ground and other states follow a different one. However the scope and severity of an potential attack and breakdown of a sector often serve as indicators which sectors need to be protected.

Not all of these sectors are especially vulnerable to cyberattacks, only those who are connected via the internet. To determine which of these sectors are connected and need special protection and should be included into a later resolution is dependent on the delegates based on their countries opinion.

b. Protection

Protection of these infrastructure sectors mentioned above means first and foremost to increase resilience and decrease attack risk of these sectors to decrease their vulnerability. To achieve sector security different means are applicable. Some examples are provided below but this list does not claim to be complete.

[2]www.dhs.gov/what-critical-infrastructure
[3]www.dhs.gov/critical-infrastructure-sectors

One of the most important is the training of personal and stakeholders working in these sectors to be more sensitive to possible threats, in our case especially the training of cyber security specialists.

To decrease the risk of attacks and implement efficient means, risk assessments in the different sectors can help identify unique weaknesses in systems which could be exploited. With the information gathered by a risk assessment measures can be adapted and implemented which tackle detected vulnerabilities in the systems tested. However depending on the specific situation in different countries not all vulnerable infrastructure sectors are state controlled. Therefore public-private partnerships are key to achieve sector security for sectors in private ownership.

Another important aspect is information and knowledge sharing across sectors between all stakeholders so that advances in one sector can be applied in other sectors to increase the efficiency of these measures. Often state institutions like Homeland Security in the U.S. service as central institutions which collect and provide knowledge to the different stakeholder. An effective response system in case of an attack is also vital to sector security. A response plan should include measures how to tackle an attack as fast and effective as possible, prevent spreading and how to ensure service continuation by sectors affected.[4]

c. Cyber Attacks

Cyberattacks in general can be defined as an illegal action with the attempt to access a computer system with the intent to cause harm. This can be done by using specific code which can alter the computer code, data or logic and therefore disrupt the system.[5] [6]

You can distinguish between different types and scales of attacks. One of the most famous types is the so called DoS-attack or Denial of Service attack. In a DoS-attack users are denied access to a service by sending requests and messages to servers

[4]www.dhs.gov/sopd
[5]www.techopedia.com/definition/24748/cyberattack
[6]www.merriam-webster.com/dictionary/cyberattack

which will use up the servers resources and therefore other users are no longer able to access the service.[7]

In 2012 for example several big US banks were targeted with a DDoS-attack, a special form of a DoS-attack, including the Bank of America, JP Morgan and others.[8]

d. Cyber Defense

There are two Cyber Defense schemes which can be employed. Most countries and companies employ a passive defense system which tries to protect and stop attacks but doesn't go any further. Active Cyber Defense (ACD) becomes increasingly important because cyber attacks become more and more sophisticated. In an ACP scheme, the attacker not only defends against an attack but also uses offensive measures to pursue the attacker and possibly recover stolen information or data. However ACD creates legal problems because defenders in there attempt to pursue the attacker may have to enter servers and computers of other companies and countries. This creates new legal challenges currently not ruled by international or national law.[9]

III. Victims and Perpetrators

The delegates should be aware that viewed from different angles different actors are affected by cyber attacks on critical infrastructure. In the case of an attack most often the service operator, so the state, a state organization, a state owned company or a private company, will be the target of the attack. More specifically there server and computer system involved in running the operations considered as critical infrastructure.

Even though the operators will be the primary target, civil society or companies depending on the functioning of the attacked service will be mainly affected by the attack. This becomes even more dangerous in a case of cascading failures, so if other critical infrastructure systems are influenced by the failure of the attacked system and also shut down.[10]

---

[7] www.techopedia.com/definition/24841/denial-of-service-attack-dos

[8] www.a10networks.com/resources/articles/5-most-famous-ddos-attacks

[9] Yagli, S & Dal, S. 2014. *Active Cyber Defense within the concept of NATO's Protection of Critical Infrastructure.* Computer and System Engineering Vol. 8 (4).

[10] Kotzanikolaou, P., Theoharidou, M & Gritzalis, D. 'Cascading Effects of Common-Cause Failures in Critical Infrastructures'. In: Butts, J. & Shenoi, S. (Eds.). 2013. *Critical Infrastructure Protection VII.* ICCIP 2013. IFIP Advances in Information and Communication Technology, Vol 417. Springer (Berlin, Heidelberg)

Tracing back the perpetrators of cyber attacks is difficult and often speculations are made because evidence and facts are rare. However, in our context of cyber attacks on critical infrastructure, two main possible actors which can act as attackers are important to us. Most CIP schemes deal with the physical threat of a terrorist attack on a critical infrastructure service. Even though there is no known case in which terrorist organizations were involved, terrorist groups definitely could start utilizing the vulnerability of critical infrastructure in the cyberspace. It is up to the delegates to decide if this scenario is realistic and probable enough to be considered.

However, the most important possible perpetrators are states attacking other states in a mean of advanced warfare. There are different prominent examples in which other states were accused of attacking critical infrastructure. In 2016 a petrochemical facility in Saudi-Arabia was attacked with the aim to cause an explosion. Based on the facts on how the attack was organized and conducted it is assumed that the attackers were supported by a government.[11]

Another famous example are attacks on the US power grid and other power facilities dating back to 2016 or possibly earlier. The US government assumes Russia to be the perpetrator of these attacks.[12]

Russia is also accused to be responsible for the hacking of computers in the German parliament. The attackers were able to infiltrate the system and had access to the data for weeks before they were discovered. The were able to extract data from the parliament network, some it may have been classified. A similar attack happened 2018 when the German Ministry of Defence and the Federal Foreign Office were infiltrated. However Russia denies any responsibilities in the attacks.[13][14]

Besides Russia, China, North Korea and Iran are suspected to build and have capabilities to attack foreign state's critical infrastructure systems.[15]

[11] www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[12] www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3

[13] www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia

[14] www.reuters.com/article/us-germany-cyber-russia/germany-says-its-government-computers-secure-after-isolated-hack-idUSKCN1GC2HZ

[15] www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#451e57f41c78

IV. Examples for National Protection Systems

Almost all countries implement Critical Infrastructure Protection schemes to ensure the continuation of basic functions of society in the case of an attack. As examples we will have a look at the strategies implemented by China, Germany and the USA.

In 2017 China introduced a new law for cybersecurity called the Cyber Security Law. The scope of Critical Infrastructure is similar to other states, however, there are two distinct differences compared to our other examples: (1) most providers are state-owned instead of private like in the US or Germany and (2) the scope also includes news agencies and social media which is unusual. Overall private-public partnerships are less important in the Chinese strategy.

The law also emphasizes that data storage and processing has to remain within China. This requirement is a special challenge for a globalized economy with more and more internet usage.[16]

Besides these specialities the strategy also involves standard requirements for education and training, sector responsibilities of the different agencies, security assessment procedures and monitoring and response procedures.[17]

The German approach is based on two strategic papers, the National Strategy for CIP from 2009 and the Cybersecurity strategy for Germany from 2016.

In the plan from 2009 the German ministry for interior lays out which infrastructure sectors qualify as critical infrastructure. It is distinguished between technical base infrastructure and socio-economic service infrastructure which is often dependent on the technical base. Besides the classification the paper also describes the possible threats for these infrastructure sectors. There are three threat categories: natural disasters, technical and human failure and terrorism and crime. It is important to note that cybersecurity in this initial plan didn't play a role and terrorism was identified as the main threat. The main strategy described in the paper include measures for prevention, reaction and sustainability. These goals are achieved with continuing information exchange between the different stakeholders, private-public partnerships and international cooperations with the EU, neighboring countries, G8 states and NATO.[18]

---

[16]de Jong-Chen, J. & O'Brien, B. 2017. *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., EU and China.* Woodrow Wilson Center Press (New York)

[17]www.twobirds.com/en/news/articles/2017/china/draft-regulations-on-critical-information-infrastructure

[18]Federal Ministry of the Interior. 2009. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Berlin

The Cybersecurity strategy from 2016 acknowledges the importance of cybersecurity for CIP. The paper recognizes cyber attacks, done by states, individuals or groups, as a significant threat to the functioning of critical infrastructure sectors. To summarize, the paper stresses the importance of private-public partnerships because some infrastructure sectors are privately controlled. The expanding connectivity of these sectors expose them to possible cyber attacks. To achieve higher cybersecurity, german IT companies need to be strengthened. Furthermore, the paper emphasizes the importance of effective prosecution of perpetrators, efficient response mechanisms and early warning systems. Similarly to the CIP Strategy from 2009, the paper acknowledges the importance of international cooperation in this matter.[19]

The last example is the scheme employed by the U.S. Department of Homeland Security since 2013. We will have a brief look at the strategy since some characteristics were already described in earlier chapters.

The US identifies 16 individual sectors which require special protection. The main strategies employed are similar to the German strategy. Public-private partnerships, education and training, information exchange and cooperation between federal, state and community governments.[20]

In the specific case of cybersecurity the 2013 issued Presidential Executive Order 13636 “Improving Critical Infrastructure Cybersecurity” tasked the U.S National Institute of Standards and Technology (NIST) to develop a framework for cybersecurity in the critical infrastructure sectors. This framework consists of three steps. A framework Core, which lays down the requirements for effective and desired activities. Framework Tiers in which the measures employed by stakeholders are ranked allowing organizations to assess and improve their measures. Framework Profiles which reflect the current implementation done by organizations and desired outcomes. These profiles therefore allow to look for possible improvements in the currently employed measures. With these standards the U.S. government wants to ensure that effective strategies are deployed by all relevant stakeholders.[21]

Overall all strategies compared show that the strategies employed by different states are heavily dependent on their economic and political system. Also the classification of critical infrastructure varies across countries and which measures and threats are

[19]Federal Ministry of the Interior. 2016. *Cyber-Sicherheitsstrategie für Deutschland 2016*. Berlin

[20]www.dhs.gov/topic/critical-infrastructure-security

[21]de Jong-Chen, J. and O’Brien, B. 2017. *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., EU and China.* Woodrow Wilson Center Press (New York)

specifically emphasized. Therefore it is important that all delegates make themselves familiar with the schemes employed by their respective country.

V. International Agreements

CIP heavily relies on international cooperation because perpetrators, especially in the context of cybersecurity, can resign in one country and commit attacks in other countries. In the case of electricity the international dependencies become clear if we look at the statistics of electricity export. Countries tend to export and import electricity and therefore an attack on a heavy exporter could have effects on countries relying on electricity imports from the attacked country. Austria for example imports around 40% of its electricity consumption.[22] [23]

Furthermore, as mentioned before, legal issues arise in the case of an attacker applying an ACD. Currently there is no national or international law or framework regulating these issues.[24]

There are different possibilities for international cooperation among countries for CIP. Often CIP cooperation happens in international organizations such as NATO, ASEAN or the EU. They all cooperate on CIP with different scope.

NATO for example is aware of the increasing threat of cyber attacks on critical infrastructure. In 2008 NATO set up the “NATO Cooperative Cyber Defense Centre of Excellence” in Tallinn which deals with threats to the cybersecurity of NATO members. Besides that NATO set up a framework in which member states can cooperate on CIP in an 2007 report, however the cooperation between members is still limited.[25] [26] [27]

VI. Role of the UN and UNSC

So far, if discussed at all, the topic of CIP was mainly discussed in the context of terrorist threats. The Counter-Terrorism Implementation Task Force (CTITF) founded in 2005 by the Secretary-General, institutionalized under the Department of Political Affairs and now part of the UN Office of Counter-Terrorism (UNOCT) since June 2017,

[22] yearbook.enerdata.net/electricity/electricity-balance-trade.html
[23] www.worlddata.info/europe/austria/energy-consumption.php
[24] Yagli, S & Dal, S. 2014. *Active Cyber Defense within the concept of NATO’s Protection of Critical Infrastructure.* Computer and System Engineering Vol. 8 (4).
[25] Yagli, S & Dal, S. 2014. *Active Cyber Defense within the concept of NATO’s Protection of Critical Infrastructure.* Computer and System Engineering Vol. 8 (4).
[26] www.nato.int/cps/en/natohq/topics_78170.htm
[27] ccdcoe.org/

consists of 38 international entities and INTERPOL and is responsible for the implementation of the UN Global Counter-Terrorism Strategy established by A/RES/60/288 in 2006.[28] [29] [30] [31]

CTITF has 12 different working groups of which one, “The Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security”, is working on the topic of CIP. This specific Working Group is working with states to establish information sharing, expand capacities in public and private sectors, facilitate public-private partnerships and improve the response and resilience capabilities.[32]

Another important resolution is S/RES/2341 which was adopted by the UNSC in February 2017. However this resolution also concentrates on the aspect of physical terrorist attacks on critical infrastructure sectors and encourages states to implement effective measures to protect these vulnerable targets.[33]

Resolution 2341 inspired two very important reports, the Counter-Terrorism Committee Executive Directorate of the UNSC (CTED) Trends Report “Physical Protection Of Critical Infrastructure Against Terrorist Attacks” which gives a compact summary on the current state of CIP in the context of terrorism.[34]

Another important report was made by the UN Office of Counter-Terrorism together with INTERPOL and the CTED. In the report “The protection of critical infrastructure protection against terrorist attacks: Compendium of good practices” the working group “The Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security” of the CTED under chairmanship of INTERPOL and UNOCT developed a Compendium of measures which can help to facilitate security for critical infrastructure sectors in the case of a terrorist attack.[35]

We encourage the delegates to read both resolutions, the first report and broadly the second report since it is 144 pages in length. Even though they are about CIP in the context of terrorism and not cybersecurity, these documents will give you a good

[28] www.un.org/counterterrorism/ctitf/en/membership-and-structure
[29] www.un.org/counterterrorism/ctitf/en/working-groups
[30] www.un.org/undpa/en/overview
[31] www.un.org/counterterrorism/ctitf/en/ctitf-office
[32] www.un.org/counterterrorism/ctitf/en/protection-critical-infrastructure-including-vulnerable-targets-internet-and-tourism-security
[33] Security Council resolution 2341, S/RES/2341 (13 February 2017), available under undocs.org/S/RES/2341(2017)
[34] CTED. 2017. *Physical Protection Of Critical Infrastructure Against Terrorist Attacks*. UN: New York
[35] United Nations, CTED & UNOCT. 2018. *The protection of critical infrastructure protection against terrorist attacks: Compendium of good practices.* UN: New York

overview over the current status of CIP in general in the UN and presents all the important players currently involved in the topic.

VII. Conclusion

CIP in the context of cybersecurity is a pressing issue recognized by most entities, national and international, dealing with CIP in the traditional way. However the UN and the UNSC never discussed or decided on a resolution on this new pressing issue. So a debate is long overdue and the UN needs to clarify its stance in this matter. Should CIP be considered a sole national issue or does the UN need to regulate and create boundaries to protect civilians?

This Study Guide gave a brief overview over the topic with examples and definitions to lay the foundation for productive debate. It is now up to the delegates to research the detailed position of their countries to engage in a fruitful debate.

VIII. Questions a Resolution should answer

- What kind of framework does the UNSC want to lay down for CIP in the context of cyberattacks?
- Which measures and which scope should be included and encouraged to be employed by member states?
- In what scope should the framework include different infrastructure sectors?
- How and in which scope should the compliance be monitored?
- In which scope should the resolution include punishment for possible perpetrators on an international level?
- How can civil society and companies be protected from the consequences of an attack?
- Which kind of attacks (perpetrators) and defense schemes should be covered by the resolution?