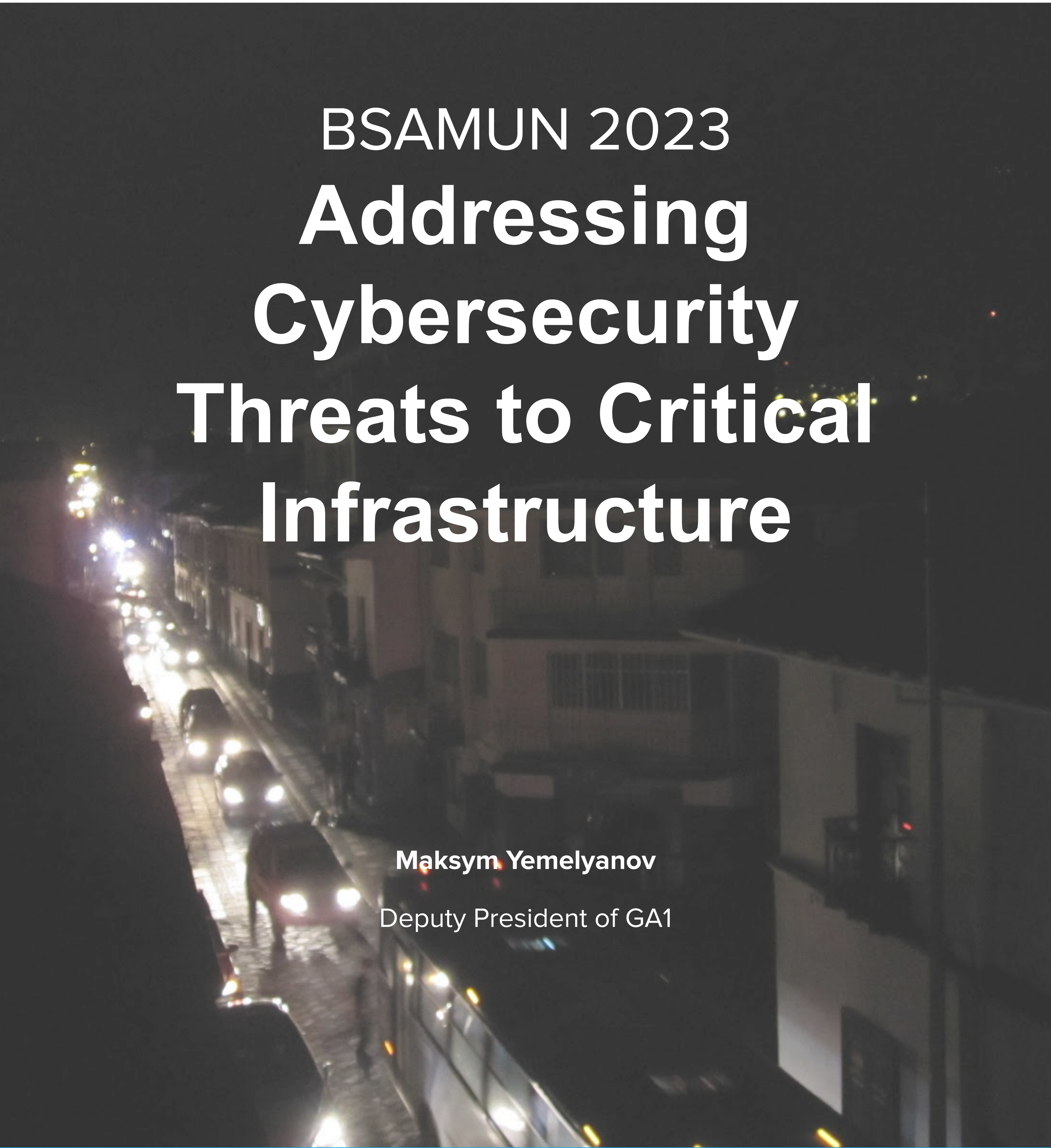

BSAMUN 2023

Addressing Cybersecurity Threats to Critical Infrastructure

Maksym Yemelyanov

Deputy President of GA1

Introduction

Cybersecurity has evolved over the last few decades, both the threats and the response to said attack. Cyber criminals have developed creative and innovative methods to target specific data frames and databases that may threaten critical infrastructure, such as power grids, transportation systems, and water treatment plants that are essential to the functioning of modern society. Cybersecurity threats to critical infrastructure can have severe consequences, such as power outages, transportation disruptions, and damage to public health and safety. Governments and organisations are taking steps to address these threats.

Definition of key terms

Cybersecurity: The security of internet-connected systems such as hardware, software, and data from cyberthreats.

Cyberattack/Cyber Crime: A crime involving a computer or computer network. The computer might have been used in the crime or it could be the target.

Critical infrastructure under threat of cyberattacks: The term "critical infrastructure" refers to the systems, networks, and assets that are required for society and the economy to function. These systems are deemed vital because their failure or interruption would have serious ramifications for public health, safety, and economic security.

Infrastructure: The basic physical and organisational structures and facilities, such as buildings, roads, and power supplies, which are needed to operate a society or enterprise.

Vulnerabilities: A weakness in the application, that could be a design defect or an implementation problem, that allows an attacker to inflict harm to the stakeholders of an application.

Hackers/cyber criminals: A person who does illegal acts using computers or the internet.

IoT devices: The Internet of Things refers to physical items equipped with sensors, processing power, software, and other technologies that connect to and share data with other devices and systems over the Internet.

Data breaches: A breach of security in which sensitive, protected, or confidential material is copied, transferred, viewed, stolen, altered, or utilised by someone who is not allowed to do so.

General Overview

Critical infrastructure such as power grids, transportation networks, and communication systems are essential to the functioning of society. However, these systems are increasingly being targeted by cyber threats, which can result in significant economic and social consequences. Cybersecurity threats to critical infrastructure can cause disruption to essential services, leading to financial losses, public safety concerns, and damage to the credibility of governments and businesses.

Cyber attacks on critical infrastructure can be carried out by a range of actors, including criminal groups, hacktivists, and nation-state actors. These attacks can take many forms, including malware, ransomware, and denial-of-service attacks. The evolving nature of cyber threats and the increasing interconnectedness of critical infrastructure systems mean that cybersecurity is an ongoing concern for governments and industry worldwide.

Cybersecurity threats to critical infrastructure are a problem because they can have serious consequences for public safety, national security, and economic stability. Critical infrastructure systems are essential for the functioning of modern societies, and disruptions to these systems can cause significant harm.

Cyber attacks on critical infrastructure can result in the loss of life, as in the case of attacks on healthcare systems or power grids. They can also lead to economic damage, such as the costs associated with recovering from a cyber attack or the loss of revenue due to disrupted services.

To address these threats, governments and industry must work together to enhance cybersecurity and build resilience against cyber attacks. This includes measures such as improving network security, increasing awareness and training for employees, and developing incident response plans. Ongoing efforts are needed to stay ahead of the evolving nature of cyber threats and protect critical infrastructure from potential attacks.

Major Parties Involved

China: China is vulnerable to cyber attacks on its critical infrastructure, including attacks on its energy, water, and transportation sectors. In recent years, there have been reports of cyber attacks on Chinese critical infrastructure, including the 2015 cyber attack on a power grid in Ukraine, which was attributed to Russian hackers but also affected Chinese grid equipment manufacturers. The Chinese government continues to work with government and industry partners to enhance cybersecurity and build resilience against cyber threats to critical infrastructure.

USA: USA is highly vulnerable to cybersecurity threats to critical infrastructure, as many of its essential services rely on interconnected computer systems. Cyber attacks on critical infrastructure can have severe consequences on public safety, economic stability, and national security. Hence willing to work toward cybersecurity.

United Kingdom: The United Kingdom is also at risk from cybersecurity threats to critical infrastructure. The UK National Cyber Security Centre (NCSC) has identified the energy, water, transport, and healthcare sectors as particularly vulnerable to cyber attacks. In recent years, there have been several high-profile cyber attacks on critical infrastructure in the UK. To address these threats, the UK government has taken several measures to enhance its cybersecurity capabilities and protect critical infrastructure.

Canada: The Canadian Centre for Cyber Security is working to prepare for and respond to cyber events and help build a stronger and more resilient cyberspace in Canada. Additionally, there are risks to Canada's national security and public safety if the threat is to the computer systems that underpin government systems, as outlined in Canada's new Cyber Security Strategy.

Russia: Russia, like many other countries, is also vulnerable to cybersecurity threats to its critical infrastructure. Cyber attacks on critical infrastructure in Russia could cause significant damage and disrupt essential services, such as energy, transportation, and healthcare. Also under a lot of pressure from other countries due to recent allegations and other claims that Russia has issued cyber attacks since the start of the renewed invasion of Ukraine.

Previous Attempts to Resolve the Issue

The UN Global Counter-Terrorism Strategy: The UN Global Counter-Terrorism Strategy emphasises the need for international cooperation to prevent and combat cyber terrorism, including cyber attacks against critical infrastructure. The strategy recognizes the growing threat of cyber attacks and emphasises the need to enhance the capacities of member states and private organisations to address the issue.

The UN Global Programme on Cybersecurity and New Technologies: The UN Global Programme on Cybersecurity and New Technologies provides technical assistance to member states to enhance their cybersecurity capacities. The program focuses on building resilience against cyber threats, including those against critical infrastructure.

The UN Office of Counter-Terrorism: The UN Office of Counter-Terrorism has several initiatives within the field of new technologies, including the Cybersecurity and New Technologies program. The program aims to enhance the capacities of member states to prevent and counter the use of information and communication technologies for terrorist purposes.

The CSA: the Cybersecurity Advisory is an organisation created in 2022 which combines all of the United States, Australia, Canada, New Zealand, and the United Kingdom to fight and protect each state that is a member of the organisation. The goal of this joint CSA is to alert enterprises that Russia's invasion of Ukraine might expose them to increasing harmful cyber activities, both inside and outside the area.

Relevant UN Programmes:

The UN Global Counter-Terrorism Strategy - 2006
The UN Global Programme on Cybersecurity and New Technologies - 2022
CSA - 2022

Possible Solutions

Addressing the problem of critical infrastructure cybersecurity threats necessitates a multifaceted strategy that combines technological, organisational, and regulatory solutions.

1. Regular risk assessments and the development of effective risk management strategies are vital for protecting critical infrastructure from cyber attacks. Identifying possible vulnerabilities, estimating the risk and effect of cyber assaults, and adopting suitable security measures are all part of this process.
2. Creating safe architecture and designs for critical infrastructure systems can help reduce the danger of cyber assaults. This involves putting in place robust access restrictions, adopting secure communication protocols, and putting encryption technology in place.
3. Frequent security testing and monitoring can aid in the identification of vulnerabilities in critical infrastructure systems as well as the detection of possible cyber assaults. This includes penetration testing, vulnerability scanning, and continuous network traffic monitoring.
4. Educating employees and stakeholders about the risks of cyber threats to critical infrastructure is essential to mitigating the problem. This includes providing cybersecurity training and awareness programs to employees, stakeholders, and the public.
5. To protect vital infrastructure, governments and commercial enterprises must collaborate to design and implement effective cybersecurity plans. This includes encouraging information exchange, improved risk management, and strengthening cybersecurity skills.
6. Cybersecurity risks to vital infrastructure are global in nature, necessitating international cooperation to properly address them. The United Nations and other international organisations are attempting to encourage international coordination and cooperation in combating cyber threats to vital infrastructure.

To summarise, dealing with cybersecurity threats to critical infrastructure necessitates a comprehensive and coordinated strategy that includes technological, organisational, and regulatory solutions. Governments, corporate entities, and international partners may collaborate to protect vital infrastructure from cyber attacks by implementing these measures.

Bibliography

1. “5 Ways to Prevent Cyberattacks on Critical Infrastructure.” Www.unearthlabs.com, www.unearthlabs.com/blogs/cybersecurity-critical-infrastructure.
2. Allianz. “Cyber Attacks on Critical Infrastructure.” AGCS Global, June 2019, www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-criticalinfrastructure.html.
3. “China Cyber Threat Overview and Advisories | CISA.” Cybersecurity and Infrastructure Security Agency CISA, www.cisa.gov/china.
4. Contributor, Company. “26 Cybersecurity Terms That Everyone Who Uses a Computer Should Know.” ThriveDX, 1 Mar. 2023, www.thrivedx.com/resources/article/25-cyber-security-terms. Accessed 10 Mar. 2023.
5. “Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA.” Www.cisa.gov, www.cisa.gov/topics/cybersecurity-best-practices.
6. Lohrmann, Dan. “NATO Countries Hit with Unprecedented Cyber Attacks.” GovTech, 4 Sept. 2022, www.govtech.com/blogs/lohrmann-on-cybersecurity/nato-countries-hit-with-unprecedented-cyber-attacks.
7. “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA.” Cybersecurity and Infrastructure Security Agency CISA, www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.
8. Security, Canadian Centre for Cyber. “Canadian Centre for Cyber Security.” Canadian Centre for Cyber Security, 28 Oct. 2022, www.cyber.gc.ca/en.
9. United Nations. “Cybersecurity | Office of Counter-Terrorism.” Www.un.org, 2020, www.un.org/counterterrorism/cybersecurity.
10. “What Is Cyber Security?” Www.ncsc.gov.uk, www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security#:~:text=Cyber%20security%20is%20how%20individuals. Ncsc.gov.uk, 2020, www.ncsc.gov.uk.