SRMUN CHARLOTTE 2021
Unity: Coming Together to Address a Changing World
March 26 - 28, 2021
sc_charlotte@srmun.org

North Atlanta Treaty Organization Update No. 1
Critical Infrastructure Security

Introduction

The Critical Infrastructure (CI) concept emerged as societies developed more advanced methods to provide assets to their expanding populations. The term CI is generally described as digital and physical assets and systems deemed so important that, if damaged, it would have a debilitating effect on safety, public health, or economic or physical security.[1] The definition of CI varies among Member States, but some of the sectors that are typically considered CI are communications, dams, emergency services, energy, food and agriculture, healthcare and public health, transportation, water and wastewater systems, and information technology.[2]

To protect its CI capabilities, the North Atlantic Treaty Organization (NATO) prioritizes civil preparedness for its Member States.[3] The success of the Alliance depends on the shared CI resources of its Member States, including railways, ports, airfields, and energy grids.[4] Under Article 3 of the North Atlantic Treaty, all NATO allies are committed to building and maintaining this national resilience, and agreed to maintaining baseline requirements for civil preparedness in seven strategic sectors: continuity of government, energy, population movement, food and water resources, mass casualties, civil communications and transport systems.[5]

As such, NATO Member State defense programs must anticipate threats from both state and non-state actors such as terrorist threats, cyber-attacks, and hybrid warfare.[6] Threats can also come in the form of natural disasters including fires, floods, and earthquakes, as well as biohazards such as the COVID-19 pandemic.[7] Member States must also adapt and respond to these different types of threats especially as they are compounded by trends that completely uproot the security environment.[8] As new technologies become more widespread, NATO allies have become more interdependent and interconnected in the financial, information, economic, and cyber domains.[9] This interconnectedness, along with the integration of technologies, benefits Member States by allowing their systems on CI to be more efficient.[10] However, the integration of sectors across Member States could expose vulnerabilities as rapid changes in any of these CI domains could severely hinder or weaken a Member State's capabilities and its ability to respond.[11]

Threats to Critical Infrastructure

---

[1] "Critical Infrastructure Security," United States Department of Homeland Security. https://www.dhs.gov/topic/critical-infrastructure-security (Accessed January 22, 2021).
[2] "Critical Infrastructure Sectors". Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/critical-infrastructure-sectors. (Accessed January 23, 2021).
[3] "Civil Preparedness," NATO. October 27, 2020. https://www.nato.int/cps/en/natohq/topics_49158.htm (Accessed March 4, 2021).
[4] "Civil Preparedness."
[5] "Civil Preparedness."
[6] "Resilience and Article 3." NATO, July 8, 2016. https://www.nato.int/cps/en/natohq/topics_132722.htm. (Accessed January 23, 2021)
[7] "Resilience and Article 3"
[8] "Resilience and Article 3
[9] "Resilience and Article 3."
[10] "Resilience and Article 3
[11] "Resilience and Article 3

One of the biggest and most notable attacks on CI was the series of attacks on the Ukrainian electric grid in December 2015.[12] A third party illegally accessed the computer and supervisory control and data acquisition (SCADA) system of Ukrainian Kyivoblenergo, a regional electric distribution company.[13] Multiple sub-stations were targeted and disconnected for three hours.[14] It was later discovered by Ukrainian Kyivoblenergo that the attack affected additional portions of the electric grid and forced workers to switch to manual mode.[15] The Ukrainian media investigated and reported that a "foreign attacker remotely controlled the SCADA distribution management system."[16] While outages were originally thought to affect approximately 80,000 Kyivoblenergo customers, it was later learned that the attacks actually impacted three other distribution companies with an estimate of 225,000 customers losing power across the region.[17] The Ukrainian government claimed that Russian security services were responsible for the incident, but these claims have not been proven.[18]
Another notable attack on CI was in Iran in June 2010.[19] At least 14 different industrial sites, including an uranium-enrichment plant, were attacked by a 500-kilobyte computer worm dubbed Stuxnet.[20] One of the key features of this attack was that a computer worm that had the ability to "spread on its own, often over a computer network," was used in the attack, unlike an attack utilizing a typical virus which must be installed on multiple devices to attack a network.[21] Stuxnet targeted Microsoft Windows systems, and sought control of programmable logic controllers.[22] It also allowed the worm's authors to spy on the industrial systems and caused systems, specifically parts in the nuclear-enrichment program, to overheat and destroy themselves without knowledge of the operators.[23] This program was so advanced that it could be spread through systems without accessing the internet and would automatically be copied onto USB thumb drives by simply plugging a USB into an infected device.[24] Secretary of Defense of United States of America (USA) Leon Panetta stated that Stuxnet could be a "cyber Pearl Harbor" if brought to the USA, as it had the capabilities to cripple power grids, derail trains, and poison water supplies in the blink of an eye.[25]

Another significant threat to CI is the recent shift in dependency on the private and commercial sectors to provide critical infrastructure, defense, and supplies.[26] In the years since the Cold War, Member State have generally reduced overall budgets, working to eliminate redundancies by transferring much of the responsibility for producing critical infrastructure and defense systems to the private sector..[27] For example, the commercial sector provides more than 30 percent of satellite communications used for defense purposes across NATO Member States, and currently, 75 percent of support for NATO operations in individual Member States are sourced from local commercial infrastructure and services.[28] While this may seem like a smart idea to reduce budgetary duplicity, privatization has also resulted in the loss of essential secondary services that, although on the surface may seem like a duplication of an already-covered expense, in reality act as emergency backup systems in times of crises.[29] This can lead to significant issues regarding CI because there are few to no backup systems capable of assuming the duties of the potentially impacted areas.

---

[12] Lee, Robert M, Michael J Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid." Industrial Control Systems SANS. E-ISAC, March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. (Accessed January 25, 2021)
[13] Lee, Robert M, Michael J Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid."
[14] Lee, Robert M, Michael J Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid."
[15] Lee, Robert M, Michael J Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid."
[16] Lee, Robert M, Michael J Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid."
[17] Lee, Robert M, Michael J Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid."
[18] Lee, Robert M, Michael J Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid."
[19] David Kushner, "The Real Story of Stuxnet," IEEE Spectrum: Technology, Engineering, and Science News, February 26, 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. (Accessed January 26, 2021)
[20] David Kushner, "The Real Story of Stuxnet."
[21] David Kushner, "The Real Story of Stuxnet."
[22] David Kushner, "The Real Story of Stuxnet."
[23] David Kushner, "The Real Story of Stuxnet."
[24] David Kushner, "The Real Story of Stuxnet."
[25] David Kushner, "The Real Story of Stuxnet."
[26] "Resilience and Article 3." NATO, July 8, 2016. https://www.nato.int/cps/en/natohq/topics_132722.htm. (Accessed January 23, 2021)
[27] "Resilience and Article 3."
[28] "Resilience and Article 3."
[29] "Resilience and Article 3."

NATO CI Resilience and Cooperation Strategies

As has been established, Protecting CI is essential to NATO and its ability to operate successfully and in a meaningful way. In efforts to maintain the protection of CI and anticipate any potential threats, NATO created the Civil Emergency Planning Committee (CEPC). The CEPC is the top NATO advisory body for protection of civilian populations, and provides NATO with expertise and guidance in "the fields of terrorism preparedness and consequence management, humanitarian and disaster response and protecting critical infrastructure."[30] The work of the CEPC touches many different facets of NATO activity. For example, in response to the COVID-19 pandemic, the CEPC is assessing and monitoring the impact the pandemic has on NATO allies and facilitating information exchange regarding best practices between them, in efforts the ensure that CI and civil preparedness are minimally impacted.[31]

Due to the multidimensional complexity of international security and the number of threats NATO faces, the top priority of NATO allies is to strengthen their resilience.[32] Many Member States do so through developing their home defense programs and honing "niche skills," like cyber defense or medical support, and combining commercial, civilian, economic, and military factors.[33] NATO does not focus on a single vulnerability and instead "contributes to protecting citizens from all potential hazards."[34] At the Summit in Warsaw (2016), Member States agreed to increase NATO's resilience to a "full spectrum of threats" and continue to improve collective and individual capabilities to combat armed attacks in any form.[35] The Committee agreed upon and passed seven baseline requirements for Member States to measure their preparedness levels.[36] These requirements serve as a baseline for operations within a Member State and address strategies needed to secure the continuity of government and critical government services, necessary energy supplies and food and water resources, resilient civil communications systems, robust transport systems, the ability to handle uncontrolled movement of people, and the ability to assist with mass casualties.[37]

Additionally, NATO strongly recommends that its allies maintain strong civilian infrastructure and supply chains, especially since during military exercises and large operations about 90 percent of military transport depends on civilian aircraft, ships, and railways.[38] NATO Deputy Secretary General Mircea Geoană stated that "there is no difference between civilian security and military strength, they're one and the same" and that NATO has been working to make infrastructure supply chains more secure.[39] For example, in 2019, NATO updated the civil communications network's baseline resilience requirements to address and include 5G internet.[40] The update specified that Member States must "conduct thorough risk and vulnerability assessments, identify and mitigate cyber threats and assess the consequences of foreign ownership control, or direct investment of critical infrastructure."[41]

---

[30] "Civil Emergency Planning Committee," NATO. https://www.nato.int/cps/en/natohq/topics_50093.htm (Accessed March 4, 2021).

[31] "Civil Preparedness," NATO. October 27, 2020. https://www.nato.int/cps/en/natohq/topics_49158.htm (Accessed March 4, 2021).

[32] "Resilience and Article 3." NATO, July 8, 2016. https://www.nato.int/cps/en/natohq/topics_132722.htm. (Accessed January 23, 2021)

[33] "Resilience and Article 3."

[34] "Resilience and Article 3."

[35] "Resilience and Article 3."

[36] "Resilience and Article 3."

[37] "Resilience and Article 3."

[38] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience." NATO, December 10, 2020. https://www.nato.int/cps/en/natohq/opinions_180067.htm?selectedLocale=en. (Accessed January 26, 2021)

[39] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[40] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[41] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

The update deemed i critical that technology like 5G be safe, secure, and trusted to guarantee security for NATO's Allies.[42]

For many years, NATO has held and completed various exercises with its allies to test the ability to handle crises involving CI.[43] These exercises involve defense infrastructure like private companies, militaries, and various Government ministries.[44] Further, to better gauge its efficacy regarding coordinated aid relief and multi-Member State support, NATO has increased the number of "life exercises" it holds.[45] These life exercises simulate scenarios in which a multinational crisis, such as the COVID pandemic, occurs, necessitating a coordinated effort to secure and distribute necessary supplies and equipment to Member States in need.[46] These exercises have revealed concerning delays in efficiency, as NATO Members were shown to be hindered by a variety of obstacles in distributing adequate supplies of high demand, low-cost items.[47]

Grey-zone Exercises are another critical example of training and testing NATO resilience and cooperation. In foreign affairs terms, warfare that is conducted in the "grey zone" of international law is activity that does not clearly cross the threshold of war but may be considered an attack, such as political warfare, cyber warfare, or hybrid warfare.[48] When conducting a Grey-zone Exercise, a Member State identifies its national security priorities and simulates a grey-zone, multifaceted attack on these priorities to determined what it would mean for the Member State, with the intent of identifying room for improvement to counter potential attacks and creating strategies to build on these capabilities by creating a competitive partnership with private sector organizations and businesses to that fosters research, innovation, and ultimately the resilience of the Member State.[49] A Grey-zone exercise involves the "exchange of information on behalf of the government and the local, the national companies," and establishes "education courses about security threats."[50] The exercises and crisis management simulations aim to point out how incoming threats can impact capital, assets, and CI throughout the Member State.[51] NATO encourages a strong and

[42] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[43] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[44] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[45] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[46] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[47] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[48] Peter Dutton, "Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?," The Conversation. June 17, 2019. https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841. (Accessed March 4, 2021).

[49] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience." NATO, December 10, 2020. https://www.nato.int/cps/en/natohq/opinions_180067.htm?selectedLocale=en. (Accessed January 26, 2021)

[50] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

[51] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."

specific focus on key areas such as expert controls, data privacy, and FDA screening in the exercises to prepare risk managers to be able to protect companies and societies as a whole.[52]

Conclusion

The effectiveness of a Member State's CI is a vital part of the day-to-day functioning of a society. CI encompasses multiple industries that are essential to individual Member States and the broader NATO Allied Forces. An attack causing a partial or complete collapse of CI assets and systems would jeopardize a Member States' ability to ensure safety, public well-being, and security. Most importantly, due to the interconnected nature of CI systems, an attack on the CI of an individual Member State could have detrimental impacts on NATO as a whole. With the possibility of systems being infected remotely and with ease, it is critical that Member States prepare for imminent threats. The security and safety of NATO allies relies on the collective action of Member States and their resilience. The interconnectedness of CI systems must be used to prepare and protect assets across allies to prevent future events as those that occurred in Ukraine and Iran.

[52] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security - Panel Discussion with NATO Deputy Secretary General, Mr. Mircea Geoană Participating in an Webinar with the American Enterprise on Resilience."