Cyberattacks on Ukraine's Power Grid Epilogue - (Russian Invasion of Ukraine 24 February 2022)

Micro Learning Module
MLM-042-C

Industry	– Power
Principal Role	– Owner
Professional Role	– All
Enterprise Phase	– Master Planning

Turn on your audio and click start to begin video

START

Author

Vytautas Butrimas

Author's presented views do not represent the official position of NATO

PRINT VERSION OF NARRATIVE

For those of you who watched the first two MLMs on Ukraine, I have added an epilogue to update you on the recent Russian invasion.
There are some valuable lessons to learn; I will briefly mention them.

Click the NEXT button when you are ready to advance to the next slide.

Russian Invasion of Ukraine: February to May 2022

- **Traditional military kinetic attacks**
  - Russian military attack and occupation of Chernobyl NPP
  - Tank fire directed at administration buildings, not the reactor

2

PRINT VERSION OF NARRATIVE

The Russian invasion of Ukraine that began on February 24th, 2022, featured both traditional military kinetic attacks against Ukrainian critical infrastructure as well as the use of cyberattacks.

The Chernobyl nuclear power plant experienced an attack and occupation by Russian military forces, which included tanks firing at the administrative parts of the plant, but did not target the reactor itself.

Russian Invasion of Ukraine: February to May 2022

- **Cyberattack against Viasat satellite terminals:**
  - Initial target was Ukraine
  - Bad firmware installed on terminals
  - Affects spread to other European countries
  - Wind farm affected in Germany
  - 5800 terminals damaged

3

PRINT VERSION OF NARRATIVE

With the start of the invasion, there were reports of cyberattacks on Viasat satellite terminals used in Ukraine. These attacks eventually spread through the Viasat control network to other customers in Europe. For example, a wind farm operator in Germany lost the communications devices used by SCADA systems to remotely monitor and control the windmills. Satellite-based communications with their large footprints on the ground, offer the advantage of providing communication links to remote and hard-to-reach locations such as a wind farm located offshore in the ocean. It is believed that the cyberattack consisted of placing a bad firmware update on the satellite communications devices which essentially required the replacement of over 5800 terminals.

Key Messages

Traditional military force has not gone out of fashion

- Cyber tactics were not the primary method for disabling critical energy and other infrastructure
- Faster to put boots on the ground

Cyberattacks were nevertheless used on satellite-based communications

- Affected the ground footprint of the satellite – Europe
- Impressive degree of precision in reaching a specific device
- Reminiscent of the NotPetya malware used against accounting software in Ukraine in 2017, which later spread to other countries and affected industrial operations.

4

PRINT VERSION OF NARRATIVE

The following are the key messages from this MLM. Sadly, the use of traditional military force on objects belonging to critical infrastructure has not gone out of fashion. In the initial actions of the war, the Russian aggressor chose not to use the advantages of stealth and deniability to disable their chosen targets. Putting boots on the ground is a much faster solution if the aggressor no longer cares if the world knows what they did; this was the case in the Russian invasion of Ukraine.

However, cyberattacks were later discovered that targeted satellite-based communications. This attack was able to spread over the ground footprint of the satellite in Europe. A key difference as opposed to a kinetic attack is the precision found in the cyber attack which targeted the satellite modems. Very interesting to note, that as with the NotPetya malware attack on Ukrainian accounting systems in 2017, which later spread to other countries and affected industrial operations, something similar seemed to happen with the satellite attacks that spread to Central Europe. Collateral damage is also a feature of cyberattacks when nations are in conflict, so be on your guard.

Further Information

Related MLMs

- MLM-042-A, *Cyberattacks on Ukraine's Power Grid 2015-2016*
- MLM-042-B, *Cyberattacks on Ukraine's Power Grid 2015-2016*

References

- Learning Map - IACS Cybersecurity for Chief Information Security Officers (CISOs)
- Ruben Santamarta, "SATCOM terminals under attack in Europe: a plausible analysis", Reversemode, March 7, 2022, https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html
- Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", Wired, March 23, 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/
- Jean-Pierre Hauet, Patrice Bock, Robert Foley, Romain Françoise, Ukrainian power grids cyberattack, InTech, Accessed 11 May 2022, https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack

5

PRINT VERSION OF NARRATIVE

For further information, take a look at the previous MLMs on earlier cyberattacks on Ukraine's power grid. There is also a learning map to provide a wider picture of what Chief Information Security Officers (CISOs) should know about industrial cybersecurity, especially if they are tasked with the responsibility of ensuring the cybersecurity of the physical operations of the enterprise. There is also an interesting article to follow up on this MLM.

Further Information

- Related MLMs
  - Cyberattacks on Ukraine's Power Grid 2015-2016 Part 2
- References:
  - https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack
  - ISA/IEC 62443 3-3 Security for industrial automation and control systems Part 3-3: System security requirements and security levels
  - Grid operators description of the attack on December 23rd https://www.youtube.com/watch?v=bV47gBsrDkc
  - https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

PRINT VERSION OF NARRATIVE

Select the Resources tab (at the top of the screen) to view and/or print this MLM, including the speaker notes. Some people like to review the slides and written narrative after listening to the micro learning module. Some like to print them and follow along as they listen to the video. It's up to you.

Vytautas Butrimas

Industrial Cybersecurity Consultant

Vytautas is a member of the International Society for Automation (ISA), Co-chair of ISA99 MLM Work Group 13, and co-moderator of the SCADASEC list. For 6 years, he served as national representative for industrial cyber security at NATO ENSEC COE, where he conducted a Cyber Risk Study of the ICS used in the NATO Central Europe Pipeline System (CEPS) and a Cybersecurity Guide for the IACS used in the NATO Pipeline System (NPS) for the NATO Petroleum Committee. He is also a member of the NATO Science and Technology Board's SAS-163 research task group preparing a report on Energy Security in an Era of Hybrid Warfare.

7

PRINT VERSION OF NARRATIVE