The Cyberwar in Ukraine

What we have learned and what we have seen so far

Johan Turell, Head of Strategy and Coordination Section

Mathias Antonsson, Cyber Strategic Analysis Lead

Department for Cybersecurity and Secure Communications

MSB Myndigheten för samhällsskydd och beredskap

Agenda

14:00-14:30: The Cyberwar in Ukraine

14:30-14:45: Q&A

14:45-14:50: Questions for the audience

14:50-15:00: Swedish fika

15:00-15:10: Reflections from the audience

15:10-15:15: Summary

15:15-15:40: SIPRI: Cyber Posture Trends in China, Russia, the United States and the European Union

15:40-15:55: Q&A

15:55-16:00: Summary

Myndigheten för samhällsskydd och beredskap

A timeline of the Cyberwar in Ukraine

Post-annexation of Crimea

- **2014**: Denial of Service attacks and defacements around the time of the illegitimate referendum on status of Crimea
- **2015**: Breaches of electricity grid operators and the spread of malware that (in one case) on the 23rd of December left 230 000 people without electricity for 1-6 hours
- **2016**: Deployment of the Industroyer malware on energy grid operators, cutting off a fifth of Kyiv's population on December 17th
- **2017**: NotPetya, probably the most destructive cyberattack ever conducted
- **2018**: Attempted attack on a chlorine distillation station in the Dnipropetrovsk region

Preamble to the full scale invasion I

- **During 2021** a great number of attempted breaches were conducted against state, regional and municipal authorities, defence companies, humanitarian organisations, critical infrastructure and nodes in digital supply chains
- **Late 2021**: Breaches to support repressive actions by an occupying force
- **13-15th of January 2022**: Defacements and attempted breaches

Preamble to the full scale invasion II

- **15th of January 2022**: The “WhisperGate” wiper was detected at several governmental agencies and a provider of it-services used by several of those agencies
- **15th of February 2022**: Waves of Denial of Service attacks, detection of breaches and a mass sms campaign
- **23rd of February 2022**: “HermeticWiper”/”FoxBlade” wiper was detected, new waves of Denial of Service attacks

The Full Scale Invasion: Late February to early March I

- **23-24th of February 2022**: New wave of Denial of Service attacks, attempts to execute “IsaacWiper”
- **24th of February 2022**: The Viasat KA-SAT satellite network was disrupted using a supply chain attack
- **25th of February 2022**: As refugees gathered at border crossings in western Ukraine, a wiper malware (probably HermeticWiper) shut down the Ukrainian border police’s information systems at a major crossing on the border to Romania

MSB Myndigheten för samhällsskydd och beredskap

The Full Scale Invasion: Late February to early March II

- **1st of March 2022**: Attempted use of the DesertBlade wiper against a major Ukrainan media company. The same day a missile attack hit a major TV tower in Kyiv
- **13th of March 2022**: CaddyWiper was detected
- **27th of March 2022**: One of Ukraine's leading broadband providers was hit by a cyberattack, reducing its network flow to only 13% of regular levels for several hours
- 800 major cyberattacks during this phase

MSB Myndigheten för samhällsskydd och beredskap

The Full Scale Invasion: The rest of 2022 I

- This phase was more characterized by a broad use of less sophisticated attacks, as well as attempts to establish access to systems in order to enable the execution of more sophisticated attacks
- **12th of April 2022**: Detection of Industroyer2 at a major electricity grid company. CaddyWiper had also been installed, probably to conceal Industroyer2 by destroying any record of it

MSB Myndigheten för samhällsskydd och beredskap

The Full Scale Invasion: The rest of 2022 II

- **Mid April – 3rd of May 2022**: Several consecutive cyberattacks were conducted against transport and logistics companies in Lviv. On the 3rd of March a missile attack hit several train stations in the area.
- **21st of July 2022**: A major Ukrainian media company was breached. From two radio stations, the attackers spread false messages claiming that President Zelensky had fallen ill and was hospitalized.

MSB Myndigheten för samhällsskydd och beredskap

How Ukraine has defended itself – and how others have defended Ukraine

Post-annexation of Crimea I

- Removal of sensitive or necessary data from data centers in the regions to better guarded servers in Kyiv
- Severed network connections between the regions
- Initiation of cooperation with the US, EU, NATO and the UK
- Establishment, in January 2016, of a National Cybersecurity Coordination Centre (NCCC)
- Establishment, in 2016, of a National Cybersecurity Strategy

MSB Myndigheten för samhällsskydd och beredskap

Post-annexation of Crimea II

- Update, in 2019, of the NCS with a focus on three pillars: Deterrence, Resilience and Interaction
- Expansion and strengthening, also in 2019, of the NCCC to implement the Interaction part of the NCS
- Expansion, partly through the help of international partners, of university education, information infrastructure upgrades, training, etc.
- Enacting, expanding and updating national cybersecurity legislation

MSB Myndigheten för samhällsskydd och beredskap

Preamble to the full scale invasion I

- Expanded international cooperation, especially with the US and the UK
  - Stronger international presence in Ukraine, helping with training, threat hunting, information sharing, networking between Ukrainian stakeholders and foreign cybersecurity companies, etc.
  - Found and neutralized the FoxBlade wiper malware in the national rail network and some rail companies
  - Set up real time threat intel sharing
  - Financial support to enable expanded security operations by private contractors
  - Provided thousands of units of communications equipment such as satellite phones and terminals

Preamble to the full scale invasion II

- New national cybersecurity legislation, modelled on the EU NIS Directive
- Enacted, on the 17th of February 2022, the Cloud Services Act which allows for the storage of sensitive and/or confidential data in cloud services – even if the servers are placed in the jurisdiction of another state

MSB Myndigheten för samhällsskydd och beredskap

After the Full Scale Invasion began

- Strengthened the physical and logical defences for data centers
- Implemented “kill switch” measures to erase data
- Prepared secure backups for a large part of the Ukrainian state’s most critical data
- Started recruiting an “IT Army” of volunteers and received support from (among others) the Belarussian “cyber partizans”
- Increased the frequencies that telecom operators could use

MSB Myndigheten för samhällsskydd och beredskap

After the Full Scale Invasion began

- Stopped blocking mobile accounts when the bills weren’t paid on time
- Blocked Russian and Belarussian SIM cards, and then allowed and surveilled them
- Started receiving Starlink terminals from SpaceX
- Received cybersecurity and resilience services by a large number of companies
- Received support in taking down attack infrastructure situated in other countries

MSB Myndigheten för samhällsskydd och beredskap

Reflections on the Cyberwar in Ukraine

Myndigheten för samhällsskydd och beredskap

How and why cyberattacks have been used

To prevent utility in Ukrainian society	To cause harm in Ukrainian society
• Disrupt the provision of essential services • Disrupt industry and other activities that are important for the national economy • Disrupt integration with the EU and relations with other Western states	• Corrupt functions in the Ukrainian state and private sector • Create distrust, fear and conflicts among the populace • Destroy infrastructure and informational assets
To prevent harm to the attacker or the attackers' employer/client	**To cause utility to the attacker or the attackers' employer/client**
• Influence the Ukrainian state to not enact policies that are counter to Russian interests • Limit Ukraines' ability to defend itself militarily • Prevent unwanted revelations or the spread of information in media or on social media	• To conduct espionage • Create sympathies for Russia and/or Russian policies

Insights on cyberattacks

- When they fail – physical attacks may follow
- May be combined with physical attacks
- May enable physical attacks
- Are often used to achieve cognitive effects
- Stocks of advanced cyber weapons run out
- The more advanced – the fewer you have ready
- Reusable/expendable cyber weapons

MSB Myndigheten för samhällsskydd och beredskap

Insights on defensive cyber strategy

- Functionality, and thus perseverance, is always the top priority
- Resilience, rather than merely robustness, is therefore key
- Non-antagonistic incidents will continue to happen, will increase in number, and will be harder to handle
- Unity of purpose is easier – but also a must
- Help will likely come – there is both sympathy and a business case
- Outside help only works when it is based on long term engagement

MSB Myndigheten för samhällsskydd och beredskap

Q&A

Myndigheten för samhällsskydd och beredskap

Question 1

The U.S. and the United Kingdom supported Ukraine more (and better) ahead of the full-scale invasion than the EU.

- To what extent should the EU engage in defence reinforcement support actions with third countries?

Myndigheten för samhällsskydd och beredskap

Question 2

The cyberwar in Ukraine has shown that even well protected organisations can fall short on stopping attacks. In the EU, we demand strong robustness and resilience for organisations. This creates barriers to market entry, and may be too expensive to some existing players – thus reducing redundancy. In war, functionality is key – so if those few players who can handle the demand should fail, we may suffer a great loss of functionality.

- Do we properly balance demands on robustness/resilience, with the ability to retain redundancy in the EU?

Myndigheten för samhällsskydd och beredskap

Swedish fika:

Be back at 15:00 (3 pm)

Myndigheten för samhällsskydd och beredskap

Reflections and summary

- To what extent should the EU engage in defence reinforcement support actions with third countries?
- Do we properly balance demands on robustness/resilience, with the ability to retain redundancy in the EU?

Myndigheten för samhällsskydd och beredskap

Thank you very much!

If you have any further questions, please contact us at:

johan.turell@msb.se

mathias.antonsson@msb.se

Myndigheten för samhällsskydd och beredskap