Swedish Civil Contingencies Agency

When war came close

Annual Report – IT Incident Reporting 2022

When war came close – Annual Report – IT Incident Reporting 2022

Photo Cover: Adobe Stock
Print: By Wind AB
Production: Advant

Publication number: MSB2208 - June 2023
ISBN: 978-91-7927-402-3

Preface

The past year has been transformative. Russia's full-scale invasion of Ukraine led to a change of course in Swedish security policy. The current world situation is serious and MSB sees shortcomings in Sweden's systematic information and cyber security work. Consequently, the work on our cyber security is more important now than ever before.

In 2022, Europe experienced its first full-scale hybrid war. A country was attacked simultaneously in both the cyber domain and with kinetic weapons. This report presents what the cyber war in Ukraine has looked like, and how development in Sweden has progressed. Overall, it reinforces old insights, but also gives us new lessons learned.

I cannot stress enough the importance of cooperation and shared learning. Together, we're strong. At the same time, MSB sees how resilience increases from good information and cyber security. The incident reports received by MSB and presented in this report also show how important it is that leading expertise is not developed at the expense of the breadth of the safety work. We have an opportunity to take advantage of the increased focus on security issues and this includes learning from the incidents that have occurred.

Some organisations are at the very beginning of their journey towards systematic and risk-based security work, while others have come much further. However, I am convinced that everyone, regardless of their status today, can further strengthen their resilience.

This report also highlights some legal issues that need to be sorted out and clarified. We will need to work together to strengthen society's ability and resilience, making it crucial that all actors in the chain take evidence-based and effective actions. We have many tools in the toolbox, but just like the emergency toolbox, the cyber toolbox must also be maintained and updated.

My hope is that through this and other publications in the field, Swedish organisations will gain the knowledge needed to be able to act to strengthen their information and cyber security work. Despite all the changes during the year, the goal remains firm, namely a secure digitalised Sweden.

Stockholm, 2023-03-15

Åke Holmgren

Director of Cyber Security and Secure Communications Department

Swedish Civil Contingencies Agency (MSB)

Innehåll

Glossary

This chapter explains the key concepts of the report.

Availability: An aspect of information security meaning, in brief, that information is accessible when requested by authorised persons.

Bots: Computers or other devices (with software) that has a specific task and are programmed to act independently, usually with network access.

Complementarity: A way to describe the duality of nature that can be bound together to a common foundation.

Confidentiality: An aspect of information security that, in brief, means that only authorised persons can access information.

Cyber-attacks: Attacks, through cyberspace, specifically directed at a nation, organisation or other actor's use of cyberspace with the intention of destroying, disabling or taking over control of a computer system.

Cyber solidarity: Solidarity, through cyberspace, between people within a group, class, nation or throughout the world prepared for mutual assistance.

Defacement: An attack that changes what meets the person who visits the targeted website. Either by changing the content of the web server or by directing the visitor to another server.

Digital supply chain: The services and infrastructures that deliver or enable the delivery of digital products that are used to establish, maintain, develop or recover an organisation's information management and information systems.

Disruption: A consequence of an incident that means that a critical infrastructure or digital services cannot be provided as intended.

Firmware: A type of software that is embedded (programmed) into hardware, such as ROM or flash memory.

Incident: An undesirable event that has occurred. In incident reporting, causes are classified according to human threats (both antagonistic threats, in the form of attacks, and non-antagonistic threats, in the form of mistakes), technical threats (in the form of system failures) or natural threats (such as weather phenomena, earthquakes, solar storms, etc.).

Information system: Systems for collecting, storing, processing and distributing information for a given purpose.

Integrity: An aspect of information security that, in short, means that information can be trusted to be accurate and not tampered with or destroyed.

Mono-dependence: An organisation is mono-dependent on (e.g.) a service when it is dependent on that service and there are no alternative services to use if the service in question cease to exist.

NIS regulation: Collective name for the Act (SFS 2018:1174), Regulation (SFS 2018:1175) and government regulations adopted in Sweden to implement the NIS Directive (EU) 2016/1148.

NIS supplier: Signifies operator of essential services and digital service provider that are subject to NIS regulation.

Ransomware: Viruses that encrypt all or part of an operation's information stored on affected information systems and make the information unavailable. Usually, ransoms are demanded to (allegedly) recover the information and/or avoid publication of the information.

Systematic information security: Working methods based on a methodology for operational risk, which aims to establish, implement, operate, monitor, review, maintain and improve the organisation's information security, i.e. the protection of information assets in terms of confidentiality, integrity and availability.

The all-hazards approach: An approach seeking to assess all risks to something to be protected, and analysing all possible causes of a risk being actualised.

Wipers: A type of malware that deletes information and actively complicates the recovery of the deleted information.

Summary

Summary

On February 24 2022, Russia began a full-scale invasion of Ukraine. For the first time since the Second World War, a large-scale war is being waged in Europe. The established security order disappeared overnight. The war came close.

This annual report is based on the IT incident reports MSB receives from government agencies and NIS suppliers. This year, new insights from the The Infosec checkup, a survey of systematic information security work in public administration, are also contributing to the content. In addition, there is a separate chapter on the cyber war in Ukraine. All in all, these elements contribute to key lessons learned and recommendations on how Swedish information and cyber security needs to be strengthened. The report is primarily intended for decision-makers, information and security managers, and external monitoring and analysis functions of both government agencies and NIS suppliers. The content may also be valuable for corresponding roles in other organisations. The annual report is also submitted to the Government of Sweden in accordance with MSB's instructions.

Russia's full-scale invasion of Ukraine has been described as the first hybrid war. Cyber-attacks played a major role, especially prior to the invasion, and the attacks confirmed the fact that an antagonist capable of conducting sophisticated attacks can subject a society to major challenges.

With extensive support from other countries and actors, Ukraine has had to deal with cyber-attacks for many years both before the large-scale invasion and since. Through targeted efforts and experience, Ukraine has built up a good resilience, which is why many cyber-attacks aimed at the country have been deterred.

The cyber warfare against Ukraine provides many lessons learned about what a strong cyber defence should be able to handle. A very likely future scenario is a sharp increase in the number of sophisticated cyber-attacks before an outbreak of war. The lessons learned from Ukraine show that a country must have good information and cyber security long before the outbreak of war to be resilient.

The state of current security policy affects Sweden's needs and ultimately MSB's role. Changes are needed in order for Sweden to have a strong cyber defence, and to be as resilient to cyber-attacks as Ukraine was at the start of the full-scale invasion. In this report, MSB presents a number of recommendations to strengthen information and cyber security. These primarily concern three things:

- MSB needs to be able to demand more information from essential societal functions and be given an expanded mandate to act on risks and vulnerabilities.
- Several investigations need to be carried out to clarify the missions and mandates of government agencies linked to cyber defence.
- In order to implement the recommendations of this report, some legislative amendments or new legislation is required.

Important news during 2022

Important news during 2022

This chapter provides brief summaries of some important news during 2022. This is to offer insight into some of the work being done in the field of cyber security.

EU cyber defence policy

Europe and Sweden are currently facing the greatest challenge to their foreign and defence policy in modern times. On November 10 2022, the European Commission presented a proposal for an EU cyber defence policy aimed at strengthening the Union's cyber defence capability, including Member States' ability to conduct joint cyber operations, strengthening coordination, information sharing and collaboration between cyber security and cyber defence.[1]

The policy is intended to lead to more effective cyber crisis management in the EU and promote joint training and exercise to strengthen collective detection capabilities. It also provides a framework for how a Member State should implement and launch the initiatives the policy advocates in order to achieve cyber solidarity. The goal is to streamline common situational reports, preparation, response and recovery in the event of a potential cyber-attack.

It is in Sweden's and the EU's interests to seek international collaboration with like-minded strategic partners to meet cyber challenges and threats. The government also stresses that the EU's strategic partnership with NATO remains of central importance, and that cooperation should therefore be characterised by complementarity.[1]

The cyber defence policy will be discussed during the Swedish EU Presidency from January 1 to June 30 2023.

New structure for Sweden's civil defence

The changing world situation has contributed to a general armament and a rebuilding of Sweden's total defence. On May 18 2022, the government presented a structural reform for emergency preparedness and civil defence, which is based on the investigation Structure for increased resilience SOU 2021:25. The new regulation entered into force on October 1 2022, where the structural

1. Joint communication on an EU cyber defence policy, https://www.riksdagen.se/sv/dokument-lagar/dokument/fakta-pm-om-eu-forslag/gemensamt-meddelande-om-en-cyberforsvarspolicy_HA06FPM30 (downloaded 03/2022).

reform is one of several components in the effort to strengthen civil defence and rebuild the total defence. The regulation aims to strengthen the whole society's ability to jointly deal with peacetime crises and improve the ability to handle heightened alert and war. It clarifies roles and mandates, and makes it easier for everyone involved to understand who is responsible for what and when.[2]

In support of the new authority structure for civil preparedness, MSB is strengthening information and cyber security work in close collaboration with other relevant government agencies. The aim is to build a resilient total defence and strengthen the ability to secure digitalisation. Part of this work is to ensure that civil defence actors, for example, have an adequate level of information and cyber security and are able to create common cyber situation reports. The systematic information and cyber security work needs a security boost for an even more robust digital society. MSB is strengthening the preparedness of the new preparedness system by, among other things, offering tools to strengthen information and cyber security, as well as through collaboration. The work is also being coordinated together with other government agencies to strengthen Sweden's collective ability to prevent, detect and manage cyber threats through the National Cyber Security Centre.

Dependence on working digital solutions can create new vulnerabilities, especially in the event of heightened alert or in case of war. Cyber-attacks on civilian targets, such as transport infrastructure, electronic communications and the energy supply, can cause severe societal disruption, affecting both civilian and military activities. In the context of a more tense security environment and demonstrated vulnerabilities among actors in the society, the society needs to strengthen its ability to withstand comprehensive disruptions caused by IT incidents. Work is being done to:

- Raise the level of organisations in society that perform the weakest in the area of information and cyber security through targeted support for the systematic information and cyber security work of these actors. This work includes follow-up.
- The ability to operationally and co-ordinatedly manage disruptions caused by IT incidents affecting society should be strengthened through exercises, support for continuity management and expanded information sharing in MSB's collaborative fora.
- The ability to use international cooperation to support information and cyber security should be strengthened.
- Preparedness is to be strengthened by the needs of total defence guiding systematic information and cyber security efforts to a greater extent than at present.
- Work on civilian and military cyber situation reports at the national level will be strengthened by developing the ability to compile cyber situation reports at the regional and sector level under heightened alert.
- The ability to secure digitalisation and innovation will be ensured through knowledge development and a more efficient supply of skills in society.

2. More information is available on MSB's website on Structural reform of emergency preparedness and civil defence, https://www.msb.se/strukturreform.

National Cyber Security Centre

The National Cyber Security Centre (NCSC-SE) is being developed according to a mission from the Government to the agencies that are jointly behind the centre. These are the Swedish National Defence Radio Establishment, the Swedish Armed Forces, MSB and the Swedish Security Service. The work is being done in close collaboration with the Swedish Post and Telecom Authority, the Swedish Police Authority and the Swedish Defence Materiel Administration. The mission of the national Cyber Security Centre is to strengthen Sweden's overall capability to prevent, detect, and manage cyber security threats.

The seven agencies that are part of the centre all have important tasks and abilities in the field of cyber security. The activities of the centre are gradually being built up and developed during 2021–2023. The cooperation between the seven government agencies in the centre strengthens the ability of the agencies to perform their respective tasks. Within the framework of the Cyber Security Centre, the agencies will coordinate efforts to prevent, detect and handle cyber-attacks and other IT incidents. They will also provide advice and support on threats, risks and vulnerabilities, and provide a national platform for collaboration and information exchange with public and private actors in the area of cyber security.

An example of an initiative launched in 2022 is the NCSC Finance forum. This collaboration forum consists of some of the centre's participating agencies, as well as government agencies and companies that are important to the financial infrastructure. Together, they will exchange information and cooperate to strengthen the financial sector's cyber security against antagonistic actors.

In-depth collaboration between MSB and the Police Authority on IT incidents

In May 2022, the Government tasked the Swedish Police Authority and MSB to deepen their cooperation regarding reported IT incidents[3] where a police report was also filed. The Government found that reporting IT incidents to MSB is of great importance, as it provides important information about threats and vulnerabilities linked to societal information and cyber security, thereby constituting an important basis for taking action to strengthen society's information and cyber security. The Government therefore also considered it important to create the conditions for this reporting to be as comprehensive as possible. In light of this, MSB and the Police Authority were given the following tasks to develop:

1. Formats and procedures that ensure that the Police Authority is notified of information received by MSB regarding IT incidents that are deemed to possibly include criminal offences.
2. A procedure to inform actors, when reporting IT incidents to the police, to also report these incidents to MSB in cases where such a reporting obligation exists for the actor.

3. Ju2016/05127, https://www.regeringen.se/regeringsuppdrag/2022/05/uppdrag-till-myndigheten-for-samhallsskydd-och-beredskap-och-polismyndigheten-att-fordjupa-samverkan-gallande-inrapporterade-och-polisanmalda-it-incidenter/ (downloaded 01/2022).

The new procedures for cooperation concerning IT incidents began to apply on 1 October 2022. When a government authority or NIS supplier reports an IT incident, MSB shares information in the scope of the operational information sharing activities conducted in the National Cyber Security Centre. When a government authority or NIS supplier files a police report on an IT incident, the Police Authority informs the reporting party of the obligation to also report the IT incident to MSB. This fulfils the objective of the in-depth collaboration on IT incidents caused by attacks.

The Infosec Checkup

In May 2021, MSB launched the The Infosec Checkup (Infosäkkollen), a follow-up structure for the systematic information security work that provides local, regional and national agencies with support in their follow-up and improvement work. The organisations were also invited to submit their responses, as a basis for overall feedback and analysis. Around half of the organisations chose to share their results, which are presented in more detail in the report "The systematic information-security work in the public sector"[4] published in 2022.

The results show that much of the public administration does not work systematically with its information security. Eight out of ten responding organisations do not reach the model's first level of four levels. The lack of breadth in this work is what is holding back the results of many organisations in The Infosec Checkup. Furthermore, it is noted that the work of the majority of the responding government agencies is behind schedule despite being subject to MSB's regulations requiring this since 2009.

The most central conclusion from MSB's analysis of the results from The Infosec Checkup is that there is a need for a general effort to strengthen systematic information security work in the public administration. A large number of organisations site resource shortages as the main obstacle to reaching higher levels of work.

MSB agrees with the assessment that many organisations, especially many municipalities, need more resources. At the same time, MSB also believes that the work can be done more effectively.

The result was expected, partially because it is the first time a measurement is made in this way and because of how The Infosec Checkup is designed, and partially because it was already known that many organisations have difficulty achieving.

4. The systematic information security efforts in public administration, Performance Reporting – Information Security Check 2021. MSB June 2022, https://rib.msb.se/filer/pdf/30002.pdf.

Reported IT incidents in 2022

Reported IT incidents in 2022

Operations that are important to the functioning of Swedish society are required by law to report IT incidents that have affected them. This chapter describes the reported incidents, the context and social consequences of the IT incidents.

Brief on IT incident reporting

From a societal and organisation perspective, it is beneficial to report IT incidents. The more information provided about incidents, the better preventive work can be developed and structured. In addition, some organisations are required to report because the activities carried out in these organisations are considered particularly critical to the functioning of our society. Reporting requirements vary depending on the regulation the organisation is affected by. The organisations that are required to report IT incidents to MSB are government agencies[5] and NIS suppliers[6].

In special circumstances, the same IT incident may need to be reported to several different government agencies. Incidents related to criminal offences must be reported both to MSB and to the Police Authority. If an incident involves an impact to personal data, it must be reported under the General Data Protection Regulation (GDPR) and, in addition to reporting to MSB, must be reported to the Swedish Authority for Privacy Protection. An incident that falls under the reporting obligation of the Protective Security Ordinance must be reported to the Swedish Security Service, and in some cases also to the Swedish Armed Forces. MSB calls on all organisations to proactively review the reporting requirements that apply to different types of IT incidents in order to be able to act quickly and correctly if and when an incident occurs.

Reported IT incidents

In 2022, a total of 330 incidents were reported to MSB, of which 231 were reported by government agencies and 99 were reported by NIS suppliers. A total of 69 government agencies and 61 NIS suppliers reported at least one incident each.

5. Ordinance on Central Government Agencies Preparedness (2022:524).
6. SFS 2018:1174 & 2018:1175.

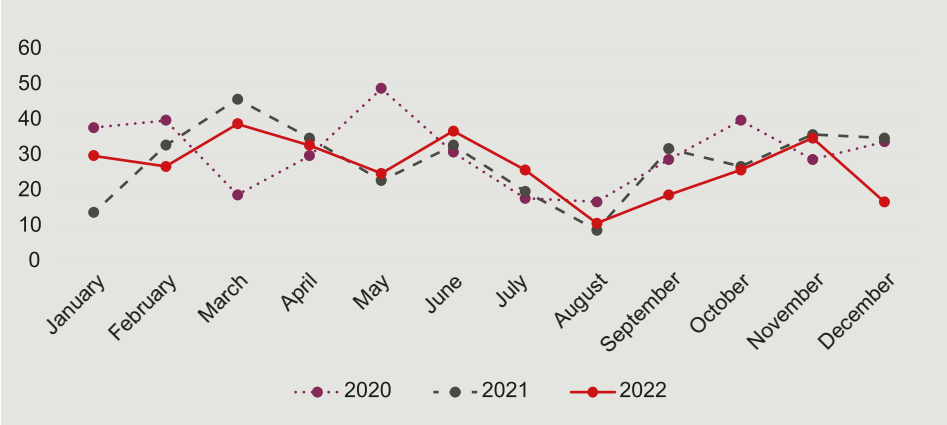
Tabell 1. Number of reported IT incidents in 2019–2022

Organisation	2022	2021	2020	2019
Government agencies	231	261	286	296
NIS suppliers	99	82	88	55
Total	**330**	**343**	**374**	**351**

Table describing the number of IT incidents reported to MSB per year during the period 2019–2022. The number of IT incidents reported by government agencies and NIS suppliers is reported separately as well as together to show the total number of incidents received.

Table 1 shows the number of reported incidents in the years 2019 to 2022. The results presented in the table show that fewer incidents were reported in 2022 than in previous years. The decrease is due solely to a decrease in the number of reports from government agencies and it is notable that the number of reports from NIS suppliers increased during the same period.

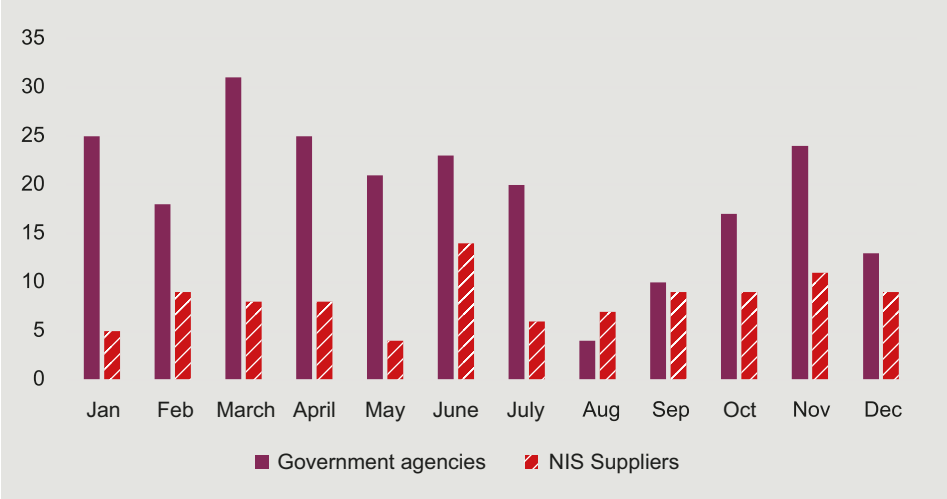
Diagram 1. Reported IT incidents per month 2020–2022



Line charts describing the number of IT incidents reported per month in the years 2020, 2021 and 2022, respectively.

Diagram 1 shows the number of reported incidents per month for the years 2020–2022. The seasonal variations for 2021 and 2022 are similar to peaks in March and June and a minimum number of reported IT incidents during August. The year 2020 differs from the later years with March as one of the months in which the least number of incidents were reported, while a sharp increase is observed in May. The annual cycle that data shows for 2021 and 2022 may be due to holiday periods with lower staffing, and/or that there are fewer incidents during holiday periods. Reporting can also go down when regular staff are replaced by extra staff who are not familiar with the procedures. The variations in 2020 could be a consequence of changes in routines and behaviours associated with the initial phase of the COVID-19 pandemic. The COVID-19 pandemic meant that organisations needed to review their priorities and that writing incident reports may have suffered due to the circumstances in March. This may have created delays in the process which then contribute to the increase in reports received in May.

Diagram 2. Reported IT incidents per month 2022 – Government agencies and NIS suppliers



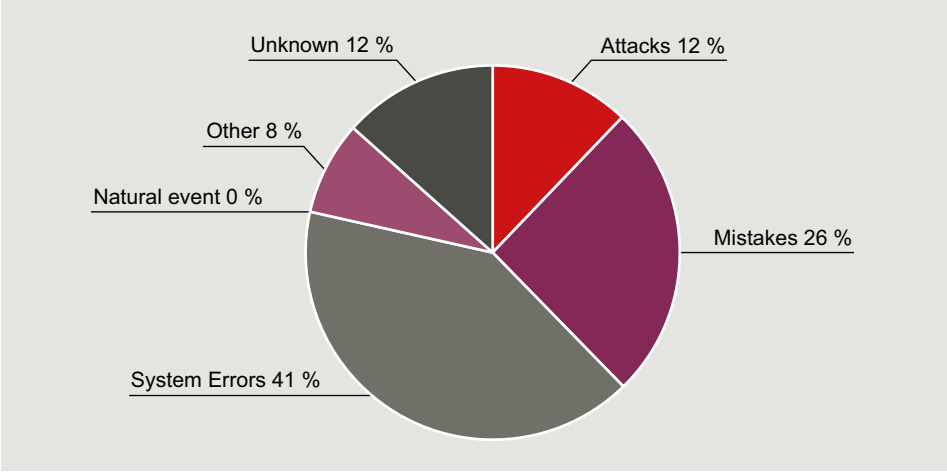
Bar chart of the number of IT incidents reported by government agencies and NIS suppliers per month in 2022.

Diagram 2 shows the number of IT incidents reported by government agencies and by NIS suppliers, on a monthly basis, in 2022. Holiday leave during the summer may explain the temporary drop in the number of reported incidents for government agencies and NIS suppliers in August and September. The increase in incoming incident reports from NIS suppliers during the month of June may be due to a serious disturbance in the TakeCare medical record system used by the majority of all health care providers in Stockholm Region.

Diagram 2 further shows that NIS suppliers incident reporting varies less from month to month than that from government agencies. This may be due to differences in the requirements regarding incident reporting for the different actors.

System error is the most common cause of incidents

Diagram 3. Distribution of reported causes of IT incidents in 2022



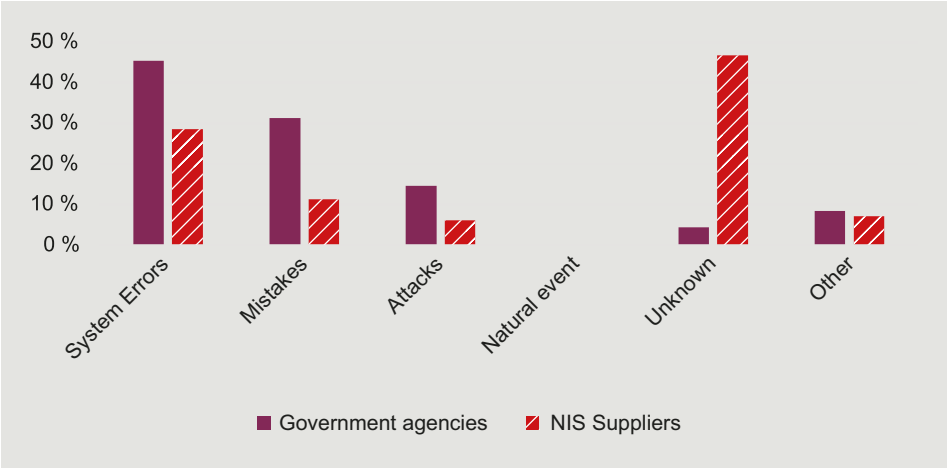
Circle diagram describing the distribution of reported causes of IT incidents based on the categories Attacks, Mistakes, System Errors, Natural Event, Other and Unknown in 2022. The category “Natural event” does not form part of the diagram because no one reported this as the cause of an IT incident in 2022.

Diagram 3 shows the percentage of incidents broken down by cause. The most common cause of reported incidents in 2022 was System errors, followed by Mistakes and then Attacks. System errors, the cause of about 41 percent of all reported incidents, include incidents in information systems that cannot be attributed to a deliberate action and stem from "bugs" in software as well as other technical complications. Mistakes, often linked to work with and updates to systems and software, were reported to be responsible for 26 percent of the reported incidents. Previous analysis shows that updates and other changes that are not made in a controlled and risk minimisation manner can increase the risk of incidents.[7] Attacks were identified as the cause of 12 percent of the reported incidents, while 8 percent ended up in the "Other" category.

The events that the reporting organisation could not place in the other categories are sorted into this "Other" category. The fact that an incident is difficult to categorise may be due, for example, to the fact that the incident reporting form does not capture all kinds of events, due to a lack of time, or to the person filling in the report having limited knowledge of the systems and/or incidents. 13 percent of the incidents were reported under the unknown category. No natural events were reported in 2022. This category is for incidents that occur due to weather events, such as flooding or lightning.

The spread of causes that are behind IT incidents highlights the importance of the all-hazards approach: an organisation needs to identify all risks associated with its IT environment, and conduct a risk analysis on how different types of incidents may affect the operations.

Diagram 4. Distribution of incidents with respect to cause for government agencies and NIS suppliers



Bar chart describing the percentage distribution of causes behind incidents in 2022 for government agencies and NIS suppliers in the categories: System Errors, Mistakes, Attacks, Natural Events, Other and Unknown, respectively.

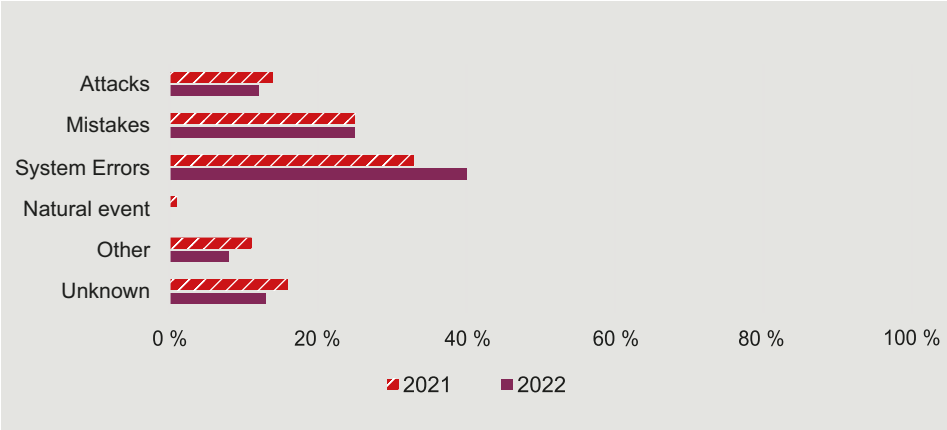
Diagram 4 shows the percentage distribution of causes behind incidents in 2022. System errors and mistakes are the largest categories for both government agencies and NIS suppliers. Diagram 4 also shows that government agencies report

7. Threats and opportunities in change management: 20 recommendations for improving information security during changes, https://www.msb.se/sv/publikationer/threats-and-opportunities-in-change-management--20-recommendations-for-improving-information-security-during-changes/.

more incidents than NIS suppliers in every category, except for the category "unknown". This may again depend on government agencies and NIS suppliers' different conditions for reporting incidents. NIS suppliers are required to report faster (within 6 hours) than government agencies (within 48 hours) in case of an indication of an incident. Lack of time may mean that the NIS supplier does not have time to identify the cause of the incident by the time that the event needs to be reported.

Natural events did not generate any incident reports in 2022. This could be because Sweden is relatively spared from extreme weather phenomena.

Diagram 5. Reported causes of IT incidents in 2021 and 2022



Horizontal bar chart describing how many reported IT incidents describe the cause of the incident as Attacks, Mistakes, System Errors, Natural Event, Other and Unknown for the years 2021 and 2022.

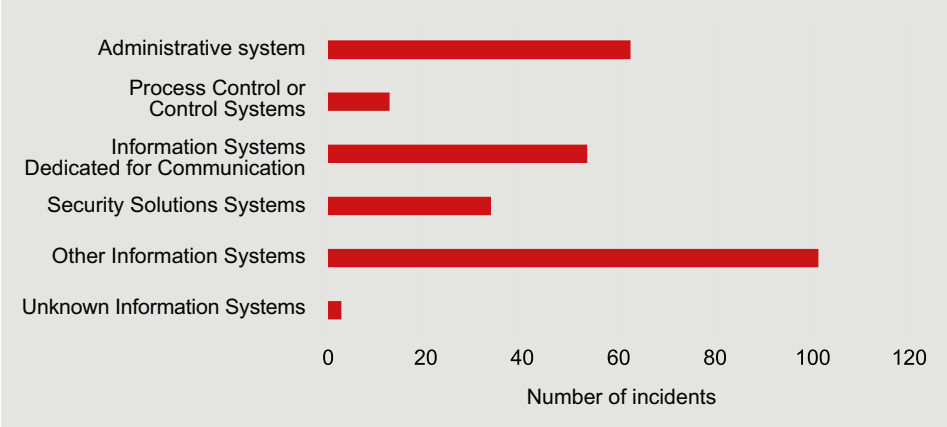
Diagram 5 shows that the distribution of the cause of incidents for 2022 is similar to that observed in 2021. System errors and mistakes are the largest categories for both years. During the initial phase of the full-scale invasion of Ukraine in 2022, it was feared that cyber-attacks would increase during the year. Despite the concern, the number of antagonistic incidents decreased in 2022 relative to 2021.

However, the report does not describe what it looks like among organisations that are not covered by the Ordinance on Central Government Agencies Preparedness or the NIS legislation.

Origin of the incidents

75 percent of the reported incidents occurred in the organisation's information system (see Diagram 6), while 10 percent of the reported incidents occurred in the peripheral environment. In the peripheral environment, it is most common that the incident affected connections such as fibre cables and other network infrastructure.

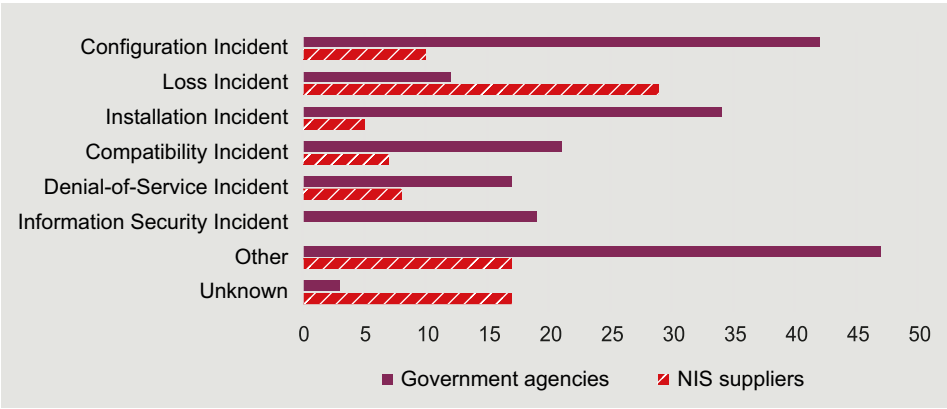
Diagram 6. Type of information system affected by IT incidents in 2022



Horizontal bar chart showing the number of incidents affecting different types of information systems. Categories that information systems are divided into include Administrative Systems, Process Control or Control Systems, Information Systems Dedicated for Communication, Security Solutions Systems, Other Information Systems and Unknown Information Systems, respectively.

Diagram 6 shows the type of information system affected by number of incidents. The 'Other Information System' category is the largest with a total of 101. The second largest is the category 'Information Systems Dedicated for Communication' and in third place are incidents in the organisation's administrative system, which may consist of medical record systems for example. Information Systems Dedicated for Communication may involve systems such as a DNS (Domain Name System).

Diagram 7. Type of IT incident in information systems in 2022 – Government agencies and NIS suppliers

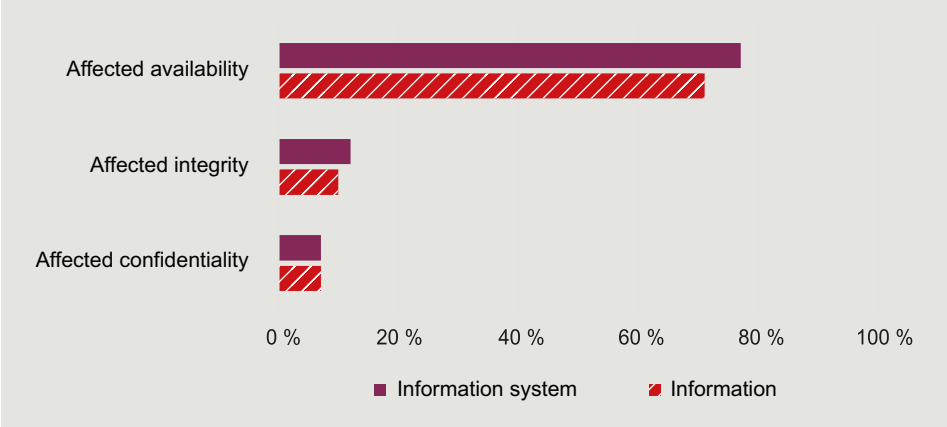


Horizontal bar chart that presents the number of reported IT incident reports that can be categorised as a particular type of incident in an information system. Included categories are Configuration Incident, Loss Incident, Installation Incident, Compatibility Incident, Denial-of-Service Incident, Information Security Incident, Other and Unknown, respectively.

Diagram 7 shows the number of times a specific type of incident was reported. According to MSB's statistics, the most incidents are placed in the categories 'Other' as well as in 'Loss Incidents' for government agencies and NIS suppliers, respectively. Loss Incidents occur when, for example, software or hardware is removed, stopped working or is destroyed. It is a category that in reporting can hide the root cause of an incident when the loss is what is noticeable: it can be difficult for an organisation to identify the origin of the incident.

Impact of incidents

Diagram 8. Percentage of IT incidents reported in 2022 affecting confidentiality, integrity or availability



Horizontal bar chart describing the percentage of reported incidents that affected information and information system Confidentiality, Integrity and Availability, respectively.

Diagram 8 presents the most common impacts, expressed as a percentage, caused by IT incidents. Based on the incident reports received by MSB, it is seen that most incidents affected the availability to both information and information systems. One reason why availability to information systems was affected to a greater extent than availability to information is that there have been alternative procedures for the handling of information.

Diagram 8 shows that incidents affecting integrity and confidentiality are uncommon.

Societal impact

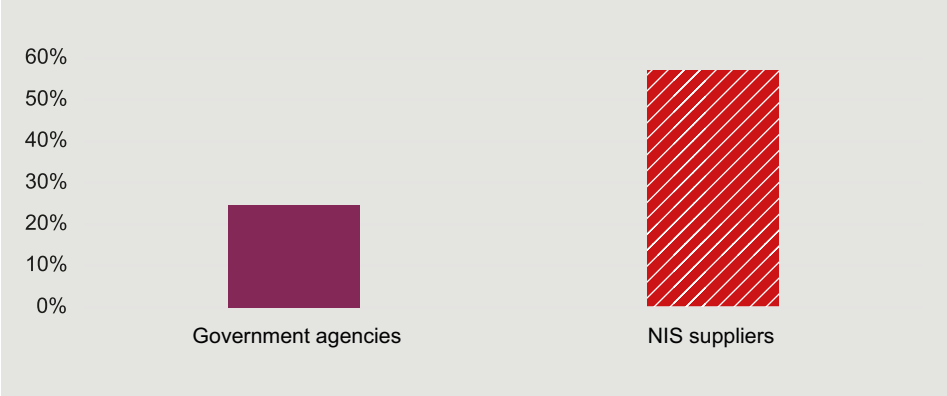
Most reported IT incidents affect availability to both information systems and information. The loss of availability to information systems by a provider of an essential service may result in different types of consequences of varying severity, depending on the type of system concerned, the disruption to which the system is subjected, and the duration of the disruption. Although a limitation in information availability may have consequences, in the vast majority of cases these types of incidents have a small impact from a societal perspective. Today, essential societal actors are largely dependent on information systems: the modern digital society can be described as redundant in the sense that there are often several actors who provide the same service. When an individual actor, such as a bank, suffers an incident affecting the availability of a service used by the public, there are other organisations that perform similar services. Thus, the impact of the incident does not need to be widespread for society as a whole.

Examples of situations where, despite a generally redundant infrastructure, an IT incident can have extensive consequences at the societal level may be when an essential service depends on one individual actor's operations, and when several providers of an essential service are vulnerable to the same type of threat.

These so-called mono-dependencies in digital supply chains[8] can potentially have major consequences from a societal perspective. Incidents in digital supply chains include both incidents when

- something that should be delivered is not delivered
- something that should not be delivered is nevertheless delivered (such as harmful code).

Diagram 9. Percentage of reported IT incidents in 2022 at suppliers – Government agencies and NIS suppliers



Bar chart describing the percentage of reports where the incident is reported to have taken place at a supplier to the reporting organisation. Government agencies and NIS suppliers are presented separately.

Diagram 9 shows that 25 percent of the incidents reported by government agencies occurred at a supplier. Among NIS suppliers, this percentage is instead 58 percent and thus accounts for over half of all disruptions that occur among these operators. A large part of these incidents, like the majority of the total number of incidents reported, were in turn caused by system errors and mistakes.

In order to avoid a widespread impact of an IT incident at a supplier, organisations, both in the public and private sectors, should take action within the framework of their systematic information security work to increase redundancy in their IT environment by avoiding mono-dependencies. Another important observation is that several organisations indicate that a lack of communication with existing suppliers has often exacerbated the disruption. In addition to increasing general redundancy, it is important to maintain functioning communication channels with suppliers and to increase their knowledge of the supply chains included in the system in several stages.

8. Read more about this in the report Digital supply chains under threat: 50 recommendations to strengthen societal security, https://www.msb.se/sv/publikationer/digital-supply-chains-under-threat--50-recommendations-to-strengthen-societal-security/.

Theme: The cyber war in Ukraine

Theme: The cyber war in Ukraine

Through strategic and systematic security work prior to and during Russia's hybrid warfare, Ukraine has managed to withstand cyber-attacks relatively well. Therefore, MSB has analysed the course of events to learn about what protection Sweden needs to build.

Hybrid warfare is depicted in this chapter based on consequences, time aspects and diversity. This includes types of attack methods and purpose perspectives so that lessons can be learned from what attacks on the cyber dimension may look like.

A pressing purpose of learning from attacks before and during the war in Ukraine is to provide a picture of what Sweden needs to be prepared and equipped for. There is much to learn from how Ukraine has worked proactively with internal as well as cross-border collaborations, exercises, training, strategies, technical and systematic searches of information systems and more. As early as 2014, following Russia's annexation of Crimea, Ukraine began to work proactively to protect its critical networks and databases in the event of cyber-attacks. These measures proved to be very useful.

Cyber-attacks have been used to influence events in Ukraine for a long time. In this in-depth analysis, MSB has studied attempted cyber-attacks targeting organisations and people in the country since the annexation of the Crimean Peninsula in 2014. The targets of the attempted attacks can be categorised into four overall categories.

Categorisation of attempted cyber-attacks targeting Ukraine	
Obstructing utility in Ukrainian society	**Causing harm in Ukrainian society**
• Disrupting or disabling an essential service. • Disrupting or disabling industry or other operations of importance to the country's economy. • Disrupting integration towards the EU and other countries in the "West".	• Corrupting functions within government and the business community. • Sowing distrust, fear and conflict. • Destroying expensive technical equipment or important information assets.
Preventing harm to the attacker or the attacker's client.	**Causing utility to the attacker or the attacker's client.**
• Influencing the Ukrainian government in order to not make choices that are not in Russia's interest. • Limiting the country's ability to defend itself militarily. • Preventing unwanted disclosures in the media or on social media.	• Espionage. • Creating sympathies for Russia or Russian positions.

Below is a selection of attempted attacks on critical operations from the period after the annexation of the Crimean Peninsula until the end of 2022. The selection is based on an external analysis from open sources. It is worth bearing in mind that Ukraine avoids exposing its own setbacks if it does not in itself create added value, and that everything that happens does not necessarily become visible to the outside world. Based on the information available to the public, the overall picture is that Ukraine has successfully resisted most of the attempted attacks. This is because the objectives of the specific cyber-attacks have not been fully achieved and because the effects of the cyber-attacks have not had extensive and serious human impact over a longer time.

Cyber-attacks before and after the full-scale invasion

Cyber-attacks have been used frequently to influence events in Ukraine since the annexation of the Crimean Peninsula in 2014.[9] In this in-depth analysis, MSB has studied cyber-attacks targeting essential functions in the country.

Retrospective look at events since 2014

Known and in many cases sophisticated attacks on Ukraine's central and essential societal functions since the annexation of the Crimean Peninsula are briefly described below.

- **2014:** Denial-of-service (DoS) attacks against and defacement (the usual content was replaced by threatening messages) of Ukrainian state authorities' websites in connection with the illegitimate referendum organised in Crimea in preparation for the official incorporation of the peninsula into the Russian Federation.
- **2015:** Intrusion and spread of malware at Ukrainian power grid operators, which in one case (on December 23) resulted in over 230,000 residents being left without electricity for 1–6 hours.[10, 11]
- **2016:** Dissemination of the harmful code Industroyer which could spread on its own in networked systems and gradually cause more damage and give the attacker access to the systems.
- **2017:** NotPetya, a particularly capable destructive code and new variant of the malware Petya discovered in 2016,[12] was planted in organisations in Ukraine via a software update in the M.E.Doc tax accounting software. Through the targeted organisations' own internal networks, the harmful code spread worldwide and encrypted the files and systems it came across. Damage equivalent to many billions of dollars occurred.

9. Greenberg, Andy. *How an Entire Nation Became Russia's Test Lab for Cyberwar*. Wired, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ (downloaded 12/2022).

10. Zetter, Kim. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Wired, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (downloaded 10/2022).

11. Miller, Christina. *Throwback Attack: BlackEnergy attacks the Ukrainian power grid*. Industrial Cybersecurity Pulse, 2021, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-blackenergy-attacks-the-ukrainian-power-grid/ (downloaded 12/2022).

12. Trellix. *What Is Petya and NotPetya Ransomware?*. 2022, https://www.trellix.com/en-us/security-awareness/ransomware/petya.html (downloaded 10/2022).

- **2018:** Failed attempt to carry out a VPNFilter cyber-attack (execution of malware on routers and storage devices by using vulnerabilities and so-called unmonitored "backdoors" to systems) on a system at Ukraine's only water and sewage treatment plant with distillation of chlorine. The attack could have led to a crash in technical processes with a risk to personnel and the general public as a result.[13] The attack was, however, able to be averted by the chlorine company's personnel in cooperation with the Ukraine's security service and other suppliers.[14]

The time before the full-scale invasion

In 2021, a large number of intrusion attempts were carried out against Ukrainian national, regional and local authorities, defence companies, humanitarian organisations and suppliers in digital supply chains of particular importance for Ukraine.[15, 16]

In February 2021, websites belonging to the Ukrainian security service and other strategically important organisations were subjected to cyber-attacks. The National Security and Defence Council of Ukraine, which was also the victim of the attack, chose not to make public details of the impact of the intrusion on Ukrainian cyber security, nor of the perpetrators of the attack.[17,18]

Towards the end of 2021, the presence of unauthorized persons in Ukraine's digital domain was reinforced. According to some analysts, part of the information gathering was to have been aimed at mapping out the population, especially in occupied areas. This mapping, in turn, was to enable the occupying power to identify opponents of the occupation.[19]

On January 13–15 2022, one month before Russia began its full-scale invasion of Ukraine, about 70 Ukrainian government websites were subjected to defacement.[20] The information normally provided on the websites was replaced with threatening messages about how the sensitive personal data of the Ukrainian

13. Cimpanu, Catalin. *Ukraine Says It Stopped a VPNFilter Attack on a Chlorine Distillation Station*. BleepingComputer, 2018, https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/ (downloaded 10/2022).

14. Leyden, John, *Ukraine claims it blocked VPNFilter attack at chemical plant.* The Register, 2018, https://www.theregister.com/2018/07/13/ukraine_vpnfilter_attack/ (downloaded 12/2022).

15. Microsoft Digital Security Unit. *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine*. Microsoft, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (downloaded 11/2022).

16. Przetacznik, Jakub and Tarpova, Simona. *Russia's war on Ukraine: Timeline of cyber-attacks*. EPRS | European Parliamentary ResearchService, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf (downloaded 10/2022).

17. Polityuk, Pavel and Zinets, Natalia. *Ukraine accuses Russian networks of new massive cyber-attacks*. Reuters, 2021, https://www.reuters.com/article/us-ukraine-cyber-idUSKBN2AM1VF (downloaded 10/2022).

18. Euractiv. *Ukraine accuses Russian networks of new massive cyber-attacks*. 2021, https://www.euractiv.com/section/europe-s-east/news/ukraine-accuses-russian-networks-of-new-massive-cyber-attacks/ (downloaded 12/2022).

19. The Associated Press. *A chilling Russian cyber aim in Ukraine: Digital dossiers*. The Associated Press. 2022-04-28, https://www.nbcnews.com/tech/security/chilling-russian-cyber-aim-ukraine-digital-dossiers-rcna26415 (downloaded 11/2022).

20. Brumfield, Cynthia. *Russia-linked cyberattacks on Ukraine: A timeline*. CSO Online. 2022-08-24, https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html (downloaded 11/2022). Andrew E. Kramer. Hackers Bring Down Government Sites in Ukraine. The New York Times. 2022-01-14, https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html (downloaded 11/2022).

people had been stolen, that this information could now be used against them and that they should prepare for "the worst".[21] On the eve of the defacement campaign, several intrusion attempts were made in order to obtain just such personal data. However, those attacks are to have largely failed.[22]

On January 15 2022, a wiperware (called "Whisper-Gate") was also discovered by government agencies in Ukraine, including those who had their web page information replaced with threatening messages. The wiper was also found at an IT service provider that many of the government agencies used.[23] The software resembled a ransomware as data was destroyed and systems were left unusable, but it contained no functions that could be used to restore infected systems.[24, 25]

On February 15 2022, nine days before the full-scale invasion, a new wave of attacks was carried out, this time in the form of denial-of-service attacks. The attacks targeted the government, banks and media companies, and resulted in some services becoming inaccessible at times. On the same day, it was revealed that intrusions were detected in the information systems of a number of government organisations.[26] The attacks were combined with a mass of text messages being sent in which it was alleged that ATMs in the country were no longer working.[27]

On February 23 2022, the day before the full-scale invasion began, a new variant of wiperware called "HermeticWiper" was discovered, which was first reported by ESET.[28] The next day, Microsoft, among others, reported on the same wiper, then under the name "FoxBlade".[29] This malware had been installed via intrusions in hundreds of systems at financial institutions and in government-contracted companies belonging to different sectors of society.[30, 31] On the same

21. Andrew E. Kramer. *Hackers Bring Down Government Sites in Ukraine*. The New York Times. 2022-01-14, https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html (downloaded 11/2022).

22. Brumfield, Cynthia. *Russia-linked cyberattacks on Ukraine: A timeline*. CSO Online. 2022-08-24, https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html (downloaded 11/2022).

23. Microsoft Digital Security Unit. *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine*. Microsoft, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (downloaded 11/2022).

24. CrowdStrike Intelligence Team. *Technical Analysis of the WhisperGate Malicious Bootloader*. Crowdstrike blog, 2022, https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/ (downloaded 11/2022).

25. Abrams, Lawrence. *Microsoft: Fake ransomware targets Ukraine in data-wiping attacks*. BleepingComputer, 2022, https://www.bleepingcomputer.com/news/security/microsoft-fake-ransomware-targets-ukraine-in-data-wiping-attacks/ (downloaded 11/2022).

26. Brumfield, Cynthia. *Russia-linked cyberattacks on Ukraine: A timeline*. CSO Online. 2022-08-24, https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html (downloaded 11/2022).

27. Vavra, Shannon. *Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In*. The Daily Beast. 2022-02-23, https://www.thedailybeast.com/cyberattacks-hit-websites-and-psy-ops-sms-messages-targeting-ukrainians-ramp-up-as-russia-moves-into-ukraine (downloaded 11/2022).

28. ESET Research. *Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper*. ESET, 2022, https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/ (downloaded 11/2022).

29. Smith, Brad. *Digital technology and the war in Ukraine*. Microsoft On The Issues. 2022-02-28, https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/ (downloaded 11/2022).

30. Microsoft Digital Security Unit. *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine*. Microsoft, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (downloaded 11/2022).

31. ESET Research. Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper. ESET Research. 2022-03-01, https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/ (downloaded 11/2022).

day denial-of-service attacks were also carried out against a large number of government authorities, financial institutions and organisations linked to Ukraine's parliament, Verkhovna Rada. Websites of the affected targets were disabled but were found to be restored within a few hours. An analysis showed that the harmful code had been created on December 28 2021, suggesting that the attack was planned well in advance.[32]

The initial phase of the full-scale invasion – late February to end of March

On February 24 2022, Russia began its full-scale invasion of Ukraine. In the hours before the invasion, there was a new wave of attempted cyber-attacks. By using intrusion into already established channels into sensitive information systems at Ukrainian authorities, yet another new type of wiperware (called "IsaacWiper") was installed and executed.[33]

On the same day, Viasat's satellite-based KA-SAT network also suffered an extensive outage. The outage was caused by a supply chain attack in which an update of firmware, which contained malware in the form of yet another wiper (called "AcidRain", at the time the seventh wiperware used in the warfare against Ukraine[34]), was distributed to and installed in special modems used to connect to the network. The attack may have been aimed at disrupting the Ukrainian armed forces' ability to lead and coordinate as their communication possibilities were degraded by the attack, but also resulted in more than 500,000 broadband customers in central Europe losing their access to the Internet, in some cases for up to two weeks.[35] In addition, the German energy company Enercon lost the ability to monitor and control 5,800 wind turbines.[36]

By February 25 2022, refugees had begun gathering at various border crossings to get out of Ukraine. At one large border crossing with Romania, a wiperware (probably HermeticWiper[37]), was used which forced the Ukrainian border police and other authorities at the border crossing to handle entry and exit with pen and paper, resulting in major delays.[38]

---

32. BBC News. *Ukraine crisis: 'Wiper' discovered in latest cyberattacks*. BBC News. 2022-02-24, https://www.bbc.com/news/technology-60500618 (downloaded 11/2022).

33. ESET Research. *Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper*. ESET Research. 2022-03-01, https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/ (downloaded 11/2022).

34. Goodin, Dan. *Mystery solved in destructive attack that knocked out >10k Viasat modems*. Ars Technica. 2022-03-31, https://arstechnica.com/information-technology/2022/03/mystery-solved-in-destructive-attack-that-knocked-out-10k-viasat-modems/ (downloaded 11/2022).

35. Pearson, James, Satter, Raphael, Bing, Christopher and Schectman, Joel. *Exclusive: U.S. spy agency probes sabotage of satellite during Russian invasion, sources say*. Reuters. 2022-03-22, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/ (downloaded 11/2022).

36. Grieg, Jonathan. *Viasat confirms report of wiper malware used in Ukraine cyberattack*. The Record. 2022-04-01, https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack/ (downloaded 2022-11-03).

37. Alspach, Kyle. *Ukraine border control hit with wiper cyberattack, slowing refugee crossing*. VentureBeat. 2022-02-27, https://venturebeat.com/security/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/ (downloaded 11/2022).

38. Berger, Miriam. 400,000 *Ukrainians flee to European countries, including some that previously spurned refugees*. The Washington Post. 2022-02-27, https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/ (downloaded 11/2022).

On 1 March 2022, a set of coordinated attacks was carried out that may have aimed at limiting ordinary Ukrainians' access to information and ability to share it. The first attack consisted of attackers attempting to use the wiperware DesertBlade in the information systems of a major media company in Ukraine. At the same time, a second attack was carried out where missiles were fired at a television tower in Kiev.[39]

On March 13 2022, the wiperware CaddyWiper was discovered in a bank's network. CaddyWiper was intended to delete user and system data to make the system unusable and the information impossible to recreate.[40]

On March 27 2022, a leading broadband provider in Ukraine was subjected to extensive cyber-attacks that rendered their services inaccessible for several hours. The broadband provider claimed that the cyber-attack entailed the biggest disruptions since the outbreak of the full-scale invasion as the network data that could be transmitted in real time dropped to 13 percent. In order to ensure that critical infrastructure and the military would not suffer disruptions, the broadband provider kept its services down for private persons and businesses during the disruptions.[41, 42]

Ukrainian authorities have reported that there were about 800 cyber-attacks against Ukrainian organisations during this phase of the war.[43]

Rest of 2022

While before and during the start of the full-scale invasion, a number of relatively sophisticated cyber-attacks were carried out against Ukraine, the period since has been marked by the widespread use of more primitive forms of attack (such as denial-of-service) as well as intrusion attempts through phishing.[44] However, some attacks of a more advanced nature have been reported:

On April 12 2022, the Ukrainian National Computer Emergency Response Team (CERT-UA) and the Slovak cyber security company ESET announced that they discovered and handled a new form of malware that can interact directly with equipment that controls electricity supply systems. The software was named Industroyer2, in reference to the software used in the 2016 cyber-attacks on the Ukrainian power grid. Industroyer2 had been installed in an electricity company's information system and included a kind of timer that allowed the software to start interacting with the power grid equipment two weeks after installation.[45] There are differing stories as to how far the attack was able to develop before

39. Microsoft Digital Security Unit. *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine*. Microsoft, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (downloaded 11/2022).

40. Osborne, Charlie. CaddyWiper: *More destructive wiper malware strikes Ukraine*. ZDNet, 2022, https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/ (downloaded 12/2022).

41. Coker, James. *Ukraine Suffers Significant Internet Disruption Following Cyber-Attack*. Infosecurity, 2022, https://www.infosecurity-magazine.com/news/ukraine-internet-disruption-cyber/ (downloaded 11/2022).

42. Vallance, Chris. *Ukraine war: Major internet provider suffers cyber-attack*. BBC, 2022, https://www.bbc.com/news/60854881 (downloaded 11/2022).

43. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

44. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. *Carnegie Endowment for International Peace*. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

45. WeLiveSecurity. *Industroyer2: Industroyer reloaded. ESET*. 2022-04-12, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (downloaded 09/2022).

it was stopped and averted. According to some information, nine transformer stations were shut down, while according to other information, nothing had time to happen at all.[46] The company that was subjected to the attack supplies electricity to approximately 2 million Ukrainians, and the consequences could have been very serious if the attempted attack had succeeded.[47] ESET also reported that Industroyer2 was used in coordination with the wiper CaddyWiper described in the previous section. By first using Industroyer2 to cause disruptions and physical damage and then CaddyWiper to destroy data, forensic analysis could have been made more difficult or even impossible. It could have prevented and greatly delayed work to develop protection against Industroyer2.[48]

On April 14 2022, Ukrainian CERT-UA warned about the trojan IcedID, which was developed to attack government agencies as well as to steal financial and banking data, began to spread by circumventing multifactor authentication among other methods. An early version of the trojan was discovered in 2017 when U.S. and Canadian banks were targeted for attack, and telecom companies, financial institutions and other organisations have since been hit globally. Whether the IcedID attack succeeded in causing damage to Ukraine's infrastructure is not clear.[49, 50]

In April, the transport and logistics sector in Lviv was attacked on a number of occasions and in various ways over a continuous period of time. On May 3, conventional missile attacks were carried out on train stations central to the transport of military and humanitarian supplies. The attack is considered to be an example of a coordinated attack involving both cyber-attacks and conventional means.[51]

On July 21 2022, the State Service of Special Communications and Information Protectorate of Ukraine (SSSCIP) announced that one of Ukraine's largest media companies, TAVR Media, was subjected to cyber-attacks.[52] The attackers attempted to take over control of all nine radio stations managed by TAVR Media, but as the company's cyber security team managed to ward off most of the attacks, only two radio stations were affected. From these two, false information was spread that Ukraine's President Zelenskyy was hospitalised. President Zelenskyy published a video of himself to dismiss the false information.[53, 54]

---

46. Greenberg, Andy. *Russia's Sandworm hackers attempted a third blackout in Ukraine*. Ars Technica. 2022-04-12, https://arstechnica.com/information-technology/2022/04/russias-sandworm-hackers-attempted-a-third-blackout-in-ukraine/ (downloaded 11/2022).

47. Wright, Rob. *Industroyer2: How Ukraine avoided another blackout attack*. TechTarget. 2022-08-10, https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack (downloaded 11/2022).

48. ESET Research. *Industroyer2: Industroyer reloaded*. WeLiveSecurity, 2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (downloaded 11/2022).

49. Bezverkhyi, Andrii. *Detecting IcedID: The Latest Campaign Against Ukrainian Government Bodies*. SOC Prime, 2022, https://socprime.com/blog/detecting-icedid-malware-the-latest-campaign-against-ukrainian-government-bodies/ (downloaded 11/2022).

50. Toulas, Bill. *Hackers target Ukrainian govt with IcedID malware, Zimbra exploits*. Bleeping Computer, 2022, https://www.bleepingcomputer.com/news/security/hackers-target-ukrainian-govt-with-icedid-malware-zimbra-exploits/ (downloaded 12/2022).

51. Smith, Brad. *Defending Ukraine: Early Lessons from the Cyber War*. Microsoft, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK (downloaded 11/2022).

52. SSSCIP Ukraine. Twitter. 2022, https://twitter.com/dsszzi/status/1550161207432298496 (downloaded 11/2022).

53. Antoniuk, Daryna. *Ukrainian radio broadcaster hacked to spread fake news about Zelensky's health*. The Record, 2022, https://therecord.media/ukrainian-radio-broadcaster-hacked-to-spread-fake-news-about-zelenskys-health/ (downloaded 11/2022).

54. Vicens, AJ. *Cyber criminals attack Ukrainian radio network, broadcast fake message about Zelensky's health*. CyberScoop, 2022, https://www.cyberscoop.com/hackers-infiltrate-ukrainian-radio-network-broadcast-fake-message-about-zelenskys-health/ (downloaded 11/2022).

On August 17 2022, the state Ukrainian company Energoatom, which operates the country's four nuclear power plants, reported that 7.25 million bots were used to carry out a denial-of-service attack on the company's website. As a result of the attacks, the electricity company's website was down for a few hours. There were no serious consequences.[55, 56]

According to reports, Ukraine has been subjected to over 1,500 cyber-attacks after the first six months of the full-scale invasion, of which more than half are to have been carried out in February and March 2022.[57]

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

Ukraine has been subjected to extensive antagonistic cyber activity for several years. The recurring attacks have spurred the country's leadership, its organisations and many citizens to strengthen information and cyber security in the country in various ways. The internal and external networks built by Ukraine over a long period of time, as well as the actors who spontaneously came to Ukraine's defence during the war, have proved invaluable. International support has played a crucial role.[58, 59]

Before 2021

Following the annexation of the Crimean Peninsula and the attempts to subversively deprive the Ukrainian state of control over the Donbass and Luhansk regions, the Ukrainian government took a number of steps to ensure that Russian authorities and organisations would not be able to access the Ukrainian state's data. Among other things, by taking control of information systems that were physically located in Crimea, or in Donbass and Luhansk. One such step was that data previously stored in the regions was moved to better protected servers in Kiev. Network connections that previously existed between the regions concerned and other parts of the country were also disconnected in order to avoid being subjected to cyber-attacks through such links.[60]

55. Antoniuk, Daryna. *Ukraine's state-owned nuclear power operator said Russian hackers attacked website*. The Record, 2022, https://therecord.media/ukraines-state-owned-nuclear-power-operator-said-russian-hackers-attacked-website/ (downloaded 11/2022).

56. RadioFreeEurope. *Ukrainian Nuclear Operator Accuses Russians Hackers Of Attacking Its Website*. RadioLiberty, 2022, https://www.rferl.org/a/ukraine-enerhoatom-hacking-attack-zaporizhzhya/31992142.html (downloaded 11/2022).

57. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

58. National Cybersecurity Cluster. National Coordination Center for Cyber Security at the National Security and Defense Council of Ukraine. *National Security and Defense Council of Ukraine*, https://cybersecuritycluster.org.ua/en/administration/ (downloaded 11/2022).

59. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

60. Geller, Eric. *Ukraine prepares to remove data from Russia's reach*. Politico. 2022-02-22, https://www.politico.com/news/2022/02/22/ukraine-centralized-its-data-after-the-last-russian-invasion-now-it-may-need-to-evacuate-it-00010777 (downloaded 11/2022).

At the same time, cooperation on security issues began with the United States, the EU, NATO and the United Kingdom.[61]

Cooperation on information and cyber security issues intensified following the cyber-attack on the Ukrainian energy companies in 2015.[62] On the Ukrainian side, a national cyber security coordination centre was established on January 27 2016 which has served as a point of contact between international partners on the one hand and national stakeholders in Ukraine on the other. Subsequently, the centre's importance to Ukrainian society's information and cyber security gradually grew, so its role and mandate were strengthened and its resources were increased in 2019.

In 2016, a national cyber security strategy was also adopted, which was then gradually implemented.[63] In connection with the increase of the cyber security coordination centre's resources in 2019, the strategy was also updated. The new strategy focuses on three pillars: deterrence, resilience and interaction, where "interaction" specifically refers to cooperation developed with NATO, the EU and the U.S. Ukrainian government representatives assess that the support received by the country has been crucial to its ability to defend itself against Russian cyber-attacks.[64, 65]

This support involved, among other things, personnel from U.S. authorities and security companies assisting Ukraine with expertise, systems, training and other aspects that strengthened the country's ability to build and configure information systems, increasing their resilience.[66] The support has also consisted of strengthening the range of training courses in the area, at Ukrainian universities for example, to assist the Ukrainian state in strengthening and updating laws and regulations, and to strengthen the networks between those with needs and those with solutions in the area. Since 2017, the United States has provided support to Ukraine in the information and cyber security field valued at more than $40 million.[67]

The period between 2021 and the full-scale invasion of 2022

In 2021, U.S. intelligence agencies in particular began to perceive a growing military threat from Russia to Ukraine, and it became increasingly clear that

61. Cameron, Lindy. United Kingdom National Cyber Security Centre. 2022. Lindy Cameron at Chatham House security and defence conference 2022. *United Kingdom National Cyber Security Centre*. 2022, https://www.ncsc.gov.uk/speech/lindy-cameron-chatham-house-security-and-defence-conference-2022 (downloaded 11/2022).

62. Sristava, Mehul, Murgia, Madhumita and Murphy, Hannah. *The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion*. The Financial Times. 2022-03-09, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471?segmentid=acee4131-99c2-09d3-a635-873e61754ec6 (downloaded 11/2022).

63. Natalia Spînu,Ukraine Cybersecurity Governance Assessment, https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf, (downloaded 11/2022).

64. National Cybersecurity Cluster. National Coordination Center for Cyber Security at the National Security and Defense Council of Ukraine. *National Security and Defense Council of Ukraine*, https://cybersecuritycluster.org.ua/en/administration/ (downloaded 11/2022).

65. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

66. Sristava, Mehul, Murgia, Madhumita and Murphy, Hannah. *The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion*. The Financial Times. 2022-03-09, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471?segmentid=acee4131-99c2-09d3-a635-873e61754ec6 (downloaded 11/2022).

67. Office of the spokesperson. U.S. Support for Connectivity and Cybersecurity in Ukraine – Fact Sheet. *U.S. Department of State*. 2022-05-10, https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/ (downloaded 11/2022).

an invasion could be on the way. In the autumn of 2021, this led to a sharp increase in the amount of people on site in the country, as well as the amount of activities they carried out there.[68] At the same time, the Ukrainian Parliament passed the Critical Infrastructure Act[69], a new piece of legislation modelled on the EU's NIS Directive.

The collaboration was concentrated on Ukrainian authorities and personnel from private companies in the country searching for, and incapacitating, ongoing intrusions and malware that had been introduced, but which, pending the large-scale invasion, had not yet been activated. Among other things, an implanted wiperware was found in information systems used in the Ukrainian train network and by Ukrainian train operators.[68]

When Microsoft discovered the wiperware they call FoxBlade in Ukrainian information systems on February 24 2021, they were able to analyse the malicious code in three hours and create signatures to detect FoxBlade. They also updated their own security software, whereby the malware could be quickly detected and handled in other information systems. The company is also supposed to have immediately contacted Ukrainian authorities, and subsequently U.S. NATO allies as well.[70]

As U.S. authorities became increasingly concerned that a large-scale invasion of Ukraine was imminent, the choice was made to deepen the information sharing and to set up special systems for that purpose.[71] Within the framework of the cooperation (which is still ongoing), which includes the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), information is shared about ongoing and potential attacks, malware and actions that can be taken. As part of the increased cooperation, the United States also sent personnel from U.S. Cyber Command to Ukraine to assist the country's equivalent authority on site.[72]

The United States Agency for International Development (USAID) has also funded supportive efforts towards companies providing critical infrastructure to search for and remove malware, handle incidents, and restore damaged information systems. USAID has also provided funding to expand the support that U.S. and Ukrainian cyber security companies can provide to Ukrainian public and private organisations, and also provided nearly 7,000 communication units such as satellite phones and terminals to the Ukrainian state and organisations in the country.[73]

---

68. Sristava, Mehul, Murgia, Madhumita and Murphy, Hannah. *The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion*. The Financial Times. 2022-03-09, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471?segmentid=acee4131-99c2-09d3-a635-873e61754ec6 (downloaded 11/2022).

69. Smilyanets, Dmitry. *A top Ukrainian security official on defending the nation against cyber-attacks*. The Record by Recorded Future. 2022-01-18, https://therecord.media/a-top-ukrainian-security-official-on-defending-the-nation-against-cyber-attacks/ (downloaded 11/2022).

70. Smith, Brad. *Digital technology and the war in Ukraine*. Microsoft On The Issues. 2022-02-28, https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/ (downloaded 11/2022).

71. Harris, Shane, DeYoung, Karen, Khurshudyan, Isabelle, Parker, Ashley and Sly, Liz. *Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion*. The Washington Post. 2022-08-16, https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/ (downloaded 11/2022).

72. Office of the spokesperson. U.S. Support for Connectivity and Cybersecurity in Ukraine – Fact Sheet. *U.S. Department of State*. 2022-05-10, https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/ (downloaded 11/2022).

73. Office of the spokesperson. U.S. Support for Connectivity and Cybersecurity in Ukraine – Fact Sheet. *U.S. Department of State*. 2022-05-10, https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/ (downloaded 11/2022).

In early 2022, the threat of invasion and the increase in antagonistic cyber activity became very tangible, leading the EU, led by Lithuania, to send a cyber rapid-response team consisting of 12 people from different EU countries. The team assisted with incident management, forensics, vulnerability analysis and scenario preparedness.[74]

Like many other countries, Ukraine had long demanded that certain data had to be stored on Ukrainian territory. On February 17 2022, one week before the full-scale invasion began, the Ukrainian Parliament passed the Cloud Service Act, which enabled the Ukrainian state to move sensitive data to cloud services, although the servers that maintain those services physically exist in another state.[75]

A special role in Ukraine's defence has been played by the country's mobile operators. A number of powerful steps were taken immediately at the start of the invasion, which would hardly have been possible without careful preparation in cooperation with others. A more detailed description of the steps taken can be found in the chapter below.

The period after the full-scale invasion

In connection with Russia's launch of the invasion of Ukraine, a large number of cyber-attacks were also carried out against Ukrainian organisations. Ukraine's CERT-UA had by then been conducting extensive activities for several months to, in cooperation with Ukrainian authorities, private organisations and international partners, handle incidents, proactively search for and remove threats, disseminate information on vulnerabilities and threats, and in other ways counter antagonistic cyber activity. After the invasion began, work continued by devoting extensive resources to providing information about threats and attacks that had been averted or handled, as well as other aspects related to the protection of Ukrainian information systems. CERT-UA has become a well-known source of cyber-security-related information about what is happening in the country.[76]

Following the annexation of the Crimean Peninsula and the subversion in Luhansk and Donetsk, data was moved from the regions to servers in the capital. Beginning before the start of the full-scale invasion, server protection was strengthened, and measures were implemented to make deletion of information impossible if the servers were to end up in the wrong hands. Ukraine also prepared backups on much of the Ukrainian state's necessary data that could be activated from a place other than Kiev should it be taken over.[77]

74. Tidy, Joe. *Ukraine: EU deploys cyber rapid-response team*. BBC. 2022-02-22, https://www.bbc.com/news/technology-60484979 (downloaded 11/2022).

75. Sayenko Kharenko. *Cloud technologies and data centres: new regulation in Ukraine*. Sayenko Kharenko. 2022-04-22, https://sk.ua/news/cloud-technologies-and-data-centres-new-regulation-in-ukraine/ (downloaded 11/2022).

76. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

77. Geller, Eric. *Ukraine prepares to remove data from Russia's reach*. Politico. 2022-02-22, https://www.politico.com/news/2022/02/22/ukraine-centralized-its-data-after-the-last-russian-invasion-now-it-may-need-to-evacuate-it-00010777 (downloaded 11/2022).

On February 24 2022, a Swedish initiative began under the leadership of an archivist at the University of Gothenburg to back up large parts of Ukraine's official websites. The initiators identified about 2,600 websites on the gov.ua domain and managed to copy two thirds of them.[78]

The Ukrainian security service SSU reported in February 2022 that the country had been subjected to massive attempts at hybrid warfare.[79] In order to strengthen its position on the cyber front, the Ukrainian Minister for Digital Transformation announced on February 26 that extensive recruitment was initiated by scientists and hackers to form Ukraine's IT army.[80] The group consists of thousands of volunteers and hacktivists and is a coordinated way for the Ukrainian government to engage in cyber-attacks against Russian targets.[81] Shortly after the creation of the IT army, a channel was put on the Telegram service to organise the group's actions. A list of over 30 targets, including Russian authorities,[82] banks and other critical infrastructure, was shared among the volunteers, consisting of hackers from all over the world.[83] In addition to Russian banks suspected to have been subjected to cyber-attacks by the IT army, there are reports that power grids and rail systems have been attacked, and that denial-of-service attacks have been used against other targets of strategic importance.[84, 85, 86]

On September 29 2022, representatives from Ukraine and the EU met to discuss cyber security issues. Among others, ENISA, CERT-EU and CERT-UA were represented. The meeting dealt with cooperation issues in the cyber security field, legislation such as the NIS Directive and Ukraine's work in adopting the EU's legal framework through cyber-security-related policies and laws. The implementation ring of Ukraine's Cyber Security Strategy 2021–2025 received attention.[87]

---

78. Dagens Nyheter. *Svenskt nätverk har säkerhetskopierat Ukrainas internet*. 2022-03-25, https://www.dn.se/sverige/svenskt-natverk-har-sakerhetskopierat-ukrainas-internet/ (downloaded 11/2022)

79. Gatlan, Sergiu. *Ukraine says it's targeted by 'massive wave of hybrid warfare'*. Bleeping Computer, 2022, https://www.bleepingcomputer.com/news/security/ukraine-says-it-s-targeted-by-massive-wave-of-hybrid-warfare-/ (downloaded 11/2022).

80. Abrams, Lawrence. *Ukraine recruits "IT Army" to hack Russian entities, lists 31 targets*. Bleeping Computer, 2022, https://www.bleepingcomputer.com/news/security/ukraine-recruits-it-army-to-hack-russian-entities-lists-31-targets/ (downloaded 11/2022).

81. Fendorf, Kyle & Miller, Jessie. *Tracking Cyber Operations and Actors in the Russia-Ukraine War*. Council on Foreign Relations, 2022, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war (downloaded 11/2022).

82. Reuters. *Official Kremlin website down amid war in Ukraine*. 2022, https://www.reuters.com/world/europe/official-kremlin-website-down-amid-war-ukraine-2022-02-26/ (downloaded 11/2022).

83. Abrams, Lawrence. *Ukraine recruits "IT Army" to hack Russian entities, lists 31 targets*. Bleeping Computer, 2022, https://www.bleepingcomputer.com/news/security/ukraine-recruits-it-army-to-hack-russian-entities-lists-31-targets/ (downloaded 11/2022).

84. Brewster, Thomas. *Moscow Exchange, Sberbank Websites Knocked Offline—Was Ukraine's Cyber Army Responsible?*. Forbes, 2022, https://www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/?sh=6933f19477ca (downloaded 11/2022).

85. Schectman, Joel. *Ukrainian cyber resistance group targets Russian power grid, railways*. Reuters, 2022, https://www.reuters.com/technology/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-2022-03-01/ (downloaded 11/2022).

86. Gatlan, Sergiu. *Russia shares list of 17,000 IPs allegedly DDoSing Russian orgs*. Bleeping Computer, 2022, https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/?&web_view=true (downloaded 11/2022).

87. EEAS, Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue. 2022-09-29. https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en (downloaded 11/2022).

In the period following the full-scale invasion, the Belarusian cyber partisans have also been involved. The group consists of hacktivists, as well as opposition activists, who formed the initiative for the grouping after the massive protests in 2020 against the Belarusian regime, as they considered the presidential election to have been manipulated.[88] In January 2022, during the intensification of the war preparations against Ukraine, the Belarusian cyber partisans alleged that they had carried out a cyber-attack against Belarus' railway system to prevent trains transporting Russian troops and artillery from carrying out attacks on Ukraine from Belarus.[89] In February 2022, the group carried out an attack on the websites used to purchase train tickets, where data in the systems may have been encrypted. While neither the extent nor the effect of the attack was widely known, the purpose was "to slow down the occupation forces and give the Ukrainians more time to fight back".[90]

As noted earlier, Viasat's satellite-based network KA-SAT was subjected to an attack during the initial phases of the invasion. The attack obstructed the Ukrainian state's and armed forces' possibilities of engaging in collaboration, and also shut down Internet access in the region. In response to that attack, as well as other physical and cyber-attacks on the telecom infrastructure, the Deputy Prime Minister of Ukraine on February 26 2022 personally appealed to the U.S. company SpaceX to deliver their Starlink terminals to Ukraine. The first deliveries arrived two days later. Starlink terminals enable Internet access over a network of about 40,000 satellites spanning the globe. SpaceX has delivered over 11,000 Starlink terminals to Ukraine where they are used for everything from collaboration within the framework of the country's defence to Internet access for individuals and organisations. As long as there is access to electricity, the spread of the Starlink terminals means that it is very difficult to take out telecommunications in the country.[91]

The Starlink operation illustrates how quickly support has been provided on occasion when suppliers and recipients have ensured in advance the capacity to fulfil an order. Another particularly significant example of this was when the Ukrainian authorities were subjected to yet another wave of denial-of-service attacks at the end of February 2022, whereby U.S. authorities contacted the security company Fortinet (which provides denial-of-service protection). That time it took only eight hours from the time the contact was made, until U.S. authorities had allocated funds and a protection against denial-of-service attacks had been installed and configured at the affected Ukrainian authorities.[92]

---

88. Antoniuk, Daryna. *How Belarusian hacktivists are using digital tools to fight back*. The Record, 2022, https://therecord.media/how-belarusian-hacktivists-are-using-digital-tools-to-fight-back/ (downloaded 11/2022).

89. Roth, Andrew. *'Cyberpartisans' hack Belarusian railway to disrupt Russian buildup*. The Guardian, 2022, https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup (downloaded 11/2022).

90. Vicens, AJ. *Belarusian hackers launch another attack, adding to chaotic hacktivist activity around Ukraine*. Cyberscoop. 2022, https://www.cyberscoop.com/belarusian-hacktivists-launch-another-attack-russia-cyber-hacktivism/ (downloaded 11/2022).

91. Miller, Christopher, Scott, Mark & Bender, Bryan. *UkraineX: How Elon Musk's space satellites changed the war on the ground*. 2022-06-08, https://www.politico.eu/article/elon-musk-ukraine-starlink/ (downloaded 11/2022).

92. Sristava, Mehul, Murgia, Madhumita and Murphy, Hannah. *The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion*. The Financial Times. 2022-03-09, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471?segmentid=acee4131-99c2-09d3-a635-873e61754ec6 (downloaded 11/2022).

Another aspect of the delivery of Starlink is that its wide use has also made Ukraine vulnerable to disruptions in the operation of the system. On October 14 2022, CNN reported that Elon Musk threatened to withdraw support for Starlink communication to Ukraine unless the U.S. military contributed millions of dollars a month to its funding.[93]

The UK also acted quickly to provide support to Ukraine. Shortly after the full-scale invasion, the UK Ukraine Cyber Programme funded by the Foreign, Commonwealth and Development Office (FCDO) began and was supported with expertise from the UK National Cyber Security Centre.

The support consisted of incident management for Ukrainian authorities (including dealing with Industroyer2), preventive measures to reduce sensitive network exposure and to harden such networks, the installation of firewalls, as well as denial-of-service protection and forensic support.[94] The support is provided in private-public collaboration between Ukrainian authorities (which provide requests and needs), UK authorities (which finance, provide advice and other support) and private cyber security companies (which provide, for example, denial-of-service protection). The support is in part reminiscent of the kind of coordination between public and private institutions that often takes place in connection with humanitarian operations.[95]

In addition to the fact that private cyber security companies have been involved in supporting Ukraine through initiatives by government organisations in the EU, the U.S., the UK and other countries, many private companies have also decided to provide support to Ukraine, sometimes without requiring compensation. In addition to those already mentioned above, BitDefender[96], Cisco[97], Cloudflare[98], Google[99], Sophos[100] and Amazon[101] can also be mentioned. The private security companies have also contributed monitoring capabilities, alarm systems, incident management, storage space, training and donations[102]. On their website, the U.S. Chamber of Commerce Technology Engagement Center

93. Marquardt, Alex. CNN. Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab. CNN 2022-10-14, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html (downloaded 11/2022).

94. Foreign, Commonwealth & Development Office, The Rt Hon Cleverly, James, MP. UK boosts Ukraine's cyber defences with £6 million support package. Gov.uk. 2022-11-01, https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package (downloaded 11/2022).

95. Beecroft, Nick. Evaluating the International Support to Ukrainian Cyber Defense. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

96. Bitdefender. Bitdefender & Romanian National Cyber Security Directorate (DNSC) Work Together in Support of Ukraine. Bitdefender, https://www.bitdefender.com/ukraine/ (downloaded 11/2022).

97. Olney, Matt. Cisco stands on guard with our customers in Ukraine. Cisco. 2022-03-03, https://blogs.cisco.com/news/cisco-stands-on-guard-with-our-customers-in-ukraine (downloaded 11/2022).

98. Prince, Matthew. Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia. Cloudflare. 2022-03-07, https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/ (downloaded 11/2022).

99. Venables, Phil. Google Cloud's security and resiliency measures for customers and partners. Google. 2022-03-03, https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-helping-those-affected-by-war-in-ukraine (downloaded 11/2022).

100. Sophos. Ukraine Crisis Resource Center. Sophos, https://www.sophos.com/en-us/content/ukraine-crisis-resource-center (downloaded 11/2022).

101. Amazon Staff. Safeguarding Ukraine's data to preserve its present and build its future. Amazon. 2022-06-09, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future (downloaded 11/2022).

102. How Tech is Supporting Ukraine, https://americaninnovators.com/news/how-tech-is-supporting-ukraine/ (downloaded 11/2022).

writes about technology companies that have helped Ukraine, among other things, with combating disinformation, measures enhancing secrecy and monetary donations. According to the article, Microsoft, Google, Facebook and Snap together have donated about $100 million in humanitarian aid and Epic Games and Xbox donated two weeks of gaming revenue from Fortnite at a value of $144 million.[103]

In addition to providing services that prevent cyber threats from causing harm, some companies have also provided services that provide redundancy and reduce the impact that would arise if the attacks were to actually result in harm. For example, several large companies have opened up large amounts of space in their cloud services so that the Ukrainian state and Ukrainian organisations will be able to back up their information.[104] This support has been made possible by the Ukrainian Cloud Service Act mentioned in the previous section. In order to facilitate the work with cloud services, several companies also provide training on how they can be used. The storage of backups in cloud services and in systems physically located in other countries (such as Poland) turned out to be a valuable step, as a Russian missile attack destroyed one of the Ukrainian state's data centres in the initial phase of the full-scale invasion. The data stored in the affected data centre was already backed up elsewhere.[105]

There are also examples of how U.S. authorities have acted proactively to defuse attempted attacks. On Wednesday, 1 June 2022, U.S. Attorney General Garland announced that they had secretly removed malicious software from computer networks around the world in order to prevent cyber-attacks. According to the Attorney General, the software in question made it possible to create "botnets", networks of private computers that, after being infected, would be controlled by an operator and used for anything from surveillance to destructive attacks. With the support of secret court decisions in the United States and with the help of the U.S. Department of Justice and the FBI, as well as governments around the world, the networks were removed from the operator's control.[106]

The fact that Ukraine has withstood the cyber-attacks on the country so well should, in addition to international aid, also be attributed to its own capabilities in the cyber area. One example of this is strong action by the country's three leading mobile operators immediately after the invasion began. These actions should be seen in the light of the fact that mobile penetration is very high in Ukraine. There are more mobile subscriptions than residents,[107] which means that mobile networks are extremely important to the country. There are three major operators, Kyivstar (26 million subscribers), Lifecell (10 million subscribers) and Vodafone Ukraine (19 million subscribers), as well as some smaller operators.

On February 24 2022, the Ukrainian telecom commission (NKRZI) bestow additional frequency bands to operators in order to better cover sparsely

103. US Chamber Technology Engagement Center. *How Tech is Supporting Ukraine*, https://americaninnovators.com/news/how-tech-is-supporting-ukraine/ (downloaded 11/2022).

104. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

105. Stupp, Catherine. Ukraine Has Begun Moving Sensitive Data Outside Its Borders. Wall Street Journal. 2022-11-09, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002 (downloaded 2022-11-09).

106. U.S. Says It Secretly Removed Malware Worldwide, Pre-empting Russian Cyberattacks. https://www.nytimes.com/2022/04/06/us/politics/us-russia-malware-cyberattacks.html (downloaded 11/2022).

107. Mobile cellular subscriptions – Ukraine, https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=UA (downloaded 11/2022).

populated areas where streams of refugees can be expected to arise.[108] On the same day, at the request of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), all operators decided to refrain from blocking accounts due to non-payments.[109] This ensured that people on the run could continue to have contact with the outside world. On the night between February 24 and 25 2022, the three operators, again at the request of NKRZI, blocked incoming roaming traffic from Russia and Belarus.[110] This blocked Russian and Belarusian users from access to Ukraine's network, thus limiting Russia's ability to inflict harm and to communicate effectively. On February 3 2022, the SSSCIP announced that all calls from Ukraine to Russia and Belarus were blocked[111], meaning that although if Russian players came across Ukrainian SIM cards, these could still not be used to call Russia or Belarus. This was later corrected and instead it was announced that the calls were regularly intercepted.[112] On March 7 2022, national roaming was introduced between the three major operators[113], which reduced the vulnerability because all subscribers could then utilize the voice and SMS services of all operators. On March 12 2022, the service offering was expanded to include data traffic over 2G and 3G[114], allowing for the use of message apps, for example.

On February 15 2022, SBU, the Ukrainian security service, announced the discovery of a so-called SIM box.[115] A SIM box is a device that contains a number of SIM cards and which may have SIM cards from various mobile operators installed, allowing it to connect calls so that they look like they come from a subscriber of one of these mobile operators. The SIM box had been used to communicate with Russian troops and to spread propaganda. Up to a thousand calls per day are reported to have been transmitted through the equipment.[116] Other SIM boxes were also discovered. For example, on February 28 2022, SBU revealed five computer networks with more than 100 SIM gateways.[117]

It is worth noting that the measures described above were implemented at the same time that the operators were subjected to extensive hybrid warfare. In an interview with Politico in September 2022, Kyivstar CEO Komarov said that large parts of the infrastructure was destroyed by physical attacks while cyber-attacks are ongoing continuously.[118]

---

108. NKEK is studying the demand of Ukrainian service providers for the spectrum, https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2250&language=uk (downloaded 11/2022).

109. Mobile operators, Ukrtelecom agree to provide communication to Ukrainians even if no funds on their account, https://interfax.com.ua/news/economic/801345.html (downloaded 11/2022).

110. Three Ukrainian mobile operators block access to their networks from Russia and Belarus, https://www.pravda.com.ua/eng/news/2022/02/26/7326240/ (downloaded 11/2022).

111. https://www.facebook.com/photo?fbid=266960745615069&set=a.234693602175117.

112. https://www.segodnya.ua/ua/strana/podrobnosti/golova-derzhspeczv-yazku-yuriy-shchigol-me-dia-ukrajini-sered-osnovnih-ciley-voroga-interv-yu-1612338.html (downloaded 11/2022).

113. Statlig tjänst för särskild kommunikation och informationsskydd i Ukraina, https://cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-pro-robotu-mobilnikh-merezh-stanom-na-11-00-10-bereznya-2022-roku (downloaded 11/2022).

114. NKEK is studying the demand of Ukrainian service providers for the spectrum, https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2273&language=uk (downloaded 11/2022).

115. https://t.me/SBUkr/3902.

116. http://www.hybertone.com/en/pro_detail.asp?proid=57.

117. Defending Ukraine together!, https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv (downloaded 11/2022).

118. Miller, Maggie, Ukraine's largest telecom stands against Russian cyberattacks. Politico 2022-09-07, https://www.politico.com/news/2022/09/07/hackers-ukraine-telecom-00055060 (downloaded 12/2022).

Lessons learned and recommendations for Sweden

Lessons learned and recommendations for Sweden

The cyber domain is and will be central to a war situation. It offers opportunities as well as risks, for our society and for the world. Although the war in Ukraine has not been directly linked to any major cyber incidents in Sweden so far, lessons can be learned from the cyber-attacks that have occurred there, as well as the effects of them.

Sweden, like the rest of the world, is undergoing an intense digitalisation process where global networks interact with local digital solutions. If critical functions have connections to a faulting link or a point of attack in this worldwide network, Swedish operations may be affected, just like many operations around the world came to be affected by, for example, the NotPetya attack in 2016. Due to the complexity of a system, the effects of cyber incidents are difficult to predict and therefore complicated to protect against. Unexpected secondary effects that are propagated and in some cases amplified when they propagate through a system pose a risk to critical infrastructure, both physical and digital, and can have significant impact in many sectors at the same time.

The consequences of incidents similar to those to which Ukraine has been subjected, both before and after the full-scale invasion, depend largely on whether safeguards are in place and how well they work. In this context, it should be pointed out that the chaotic circumstances prevailing in a war situation contribute to further complications. If many functions, mechanical, technical and/or in the form of manpower, go down at the same time, disruptions can be difficult to track and to fix.

Below are some key lessons for Sweden that can be learned from the The Infosec Checkup, the reported incidents and the cyber war in Ukraine. These are particularly relevant if Sweden finds itself in a situation of heightened alert or war.

Lesson 1: Together, we're strong

Ukraine has received extensive support from the outside world in all aspects of the cyber warfare. This has been crucial for the country to succeed so well in withstanding the cyber-attacks that have been directed against them. The success can largely be attributed to the careful preparations for cooperation under way for a long time that intensified in connection with the Russian occupation of Crimea in 2014.

However, it takes time to establish cooperation and there are a number of conditions that must be met in order for it to be possible to receive outside support. For it to work, a trusting relationship is required where contact channels and procedures are established and practised. The pure technical difficulty involved should also not be underestimated. The complexity of IT environments is often high and they require in-depth knowledge to be able to navigate, and to securely optimise the system. This makes it clear that cooperation should also be established at the operational level.

It is also important to conduct an informed risk assessment. A deep technical, and perhaps automated, support requires very extensive access and thereby creates risks that potential new attack vectors can arise. Here, confidence in the person who will provide the support is absolutely crucial.

Cooperation between the public and private sectors

In connection with the full-scale invasion of Ukraine, we have seen Ukrainian companies interacting with each other and with authorities to defend Ukraine, and they have apparently done so with good results. However, it is no given that this will be the case should a corresponding war situation arise in Sweden, as there is sometimes a conflict of interest between the primary objectives of private companies and the objectives of national security.

Support may therefore have to be designed to suit different organisations or functions. When it comes to support between authorities, the relationships are simpler than between independent companies. Companies also have objectives other than societal utility to take into account. For example, conflicts may arise between the goal of getting to the bottom of the causes of an intrusion attempt and the goal of creating profits for shareholders. In addition, comprehensive legal regulations and mandatory audits are rarely in line with what companies want. Another inhibitor may be the fear of sanctions in the event of a lack of security being detected in connection with an operation.[119] Furthermore, companies may be subject to legal requirements in several jurisdictions that make cooperation with external experts difficult. This means that certain legislation may need to be reviewed, both for companies and authorities, in order to allow for the appropriate sharing of personal data and other sensitive information.

Consideration needs to be given to the fact that a company's main task is to generate value for its owners, which is not compatible with exposing the company's assets to war risks that could be avoided. This means that services provided by companies may be shut down, or that production may be moved elsewhere. Companies may also be under pressure from other countries to relocate their activities, especially if that activity is considered to be of strategic importance to those countries. This becomes particularly clear to companies that do not have their head office in Sweden or have a significant share of foreign ownership.

One factor that further complicates the picture is that even those companies that choose to stay in Sweden may have problems operating if they have dependencies on other companies that in turn choose to terminate their operations in Sweden or who for other reasons no longer can or want to supply the necessary inputs and services to Swedish companies.

119. Sipri and MSB 2020: *Cyber-incident management – Identifying and Dealing with the Risk of Escalation*. https://sipri.org/sites/default/files/2020-11/sipripp55.pdf.

Cooperation in Sweden

Our society has a fundamental resilience, and society's ability to deal with crises was strengthened during the COVID-19 pandemic. However, as has been shown above, there are also a lot of shortcomings and vulnerabilities that need to be addressed and it is not only the large-scale Russian invasion of Ukraine that makes it urgent. We need to be prepared for a series of events that can affect us, ranging from new pandemics, extreme weather and major industrial accidents to terrorist attacks and sabotage. Preparedness needs to be taken into account in all planning of essential societal functions.

The purpose of the new authority structure[120] is to make the division of responsibilities clearer, the contact pathways straighter and the cooperation closer, and to make it easier for essential societal functions to understand how they can contribute to strengthening preparedness in society. The government agencies with sector responsibility prepare to be able to act quickly and in a coordinated manner in the event of peacetime crisis situations, heightened alert and war. The contingency agencies have specific tasks in addition to those of all national agencies. They should also serve as examples and work to ensure that essential societal functions develop their capabilities in these respects. In the event of heightened alert, the contingency agencies must focus their activities on tasks relevant to total defence.

Swedish society depends on resilient digital solutions. Consequently, good cyber security is a prerequisite in order for essential societal functions to work. The systematic work on information and cyber security has improved, but the rapid digitalisation creates new vulnerabilities. Society needs to strengthen its ability to withstand major disruptions caused by IT incidents for whatever reason. Together with other government agencies, MSB also coordinates the work to strengthen Sweden's collective ability to prevent, detect and manage cyber threats through the National Cyber Security Centre.

EU

Sweden's with other EU Member States contributes to strengthening Swedish information and cyber security. Some of the most central collaborations are exemplified by the NIS Cooperation Group, the CSIRT network and EU-CyCLONe. Co-operation at the policy level also strengthens common information and cyber security. The EU Cyber Defence Policy, the Cyber Resilience Act and the AI Regulation are particularly key examples.

The NIS Cooperation Group supports and facilitates strategic cooperation and information exchange and strengthens confidence and trust between Member States. The Cooperation Group has the possibility to invite to discussions relevant Union institutions, bodies, offices and agencies dealing with cyber security issues, such as the European Parliament, Europol and the European Data Protection Board.

The CSIRT network has been set up to help strengthen confidence and trust and promote rapid and effective operational cooperation between Member States. The CSIRT network consists of representatives of the CSIRT units designated or established in accordance with the NIS Directive and the CERT-EU incident management organisation for Union institutions, bodies and agencies.

120. More information is available on MSB's website on Structural reform of emergency preparedness and civil defence, https://www.msb.se/strukturreform.

EU-CyCLONe shall act as an intermediary between the technical and political levels during large-scale cyber security incidents and crises and to strengthen cooperation at the operational level and support decision-making at the political level.

In order to facilitate cross-border cooperation and communication, each Member State has also designated a single contact point responsible for coordinating issues relating to the security of network and information systems and cross-border cooperation at the Union level.

NATO

Sweden currently has individual cooperation with NATO within the framework of the Partnership for Peace. The starting point for cooperation is strengthened emergency preparedness and civil defence. Some examples of areas of cooperation to ensure essential societal functions in the event of a potential crisis are food and energy supply, as well as safe transportation.[121]

In the event of membership, Sweden is expected to participate fully in NATO's civil preparedness structures and contribute to the development of society's resilience, both as a national responsibility and as part of the collective commitment. NATO's seven fundamental capabilities are very similar to the areas that are prioritised for the development of our Swedish civil defence.

During 2023, Sweden will pursue the aim of Swedish participation with a focus on civilian preparedness work. Sweden will seek an increased presence in all relevant NATO structures for a strengthened political dialogue and an increased exchange of information. MSB will continue to maintain an overall picture of Swedish participation in this work and is responsible for civil defence issues.[122]

→ Recommendations

Ukraine has received extensive support from the outside world in all aspects of cyber warfare, which has been crucial to the country's success in resisting cyber-attacks as well as it has. There are a number of conditions that need to be met for it to be possible to receive outside support; these are the same for Sweden as for Ukraine. The following preparatory work is important in order to:

- ✓ Establish and strengthen collaborations in cyber security areas both nationally and with strong international partners.
- ✓ Create procedures for how international assistance can be received.
- ✓ Create procedures to be able to share intelligence information with international partners.
- ✓ Plan states of readiness in organisations responsible for critical infrastructure.

121. Ju2021/00361 Raminstruktion för det svenska civila beredskapsarbetet inom ramen för Nato/PFF, https://www.msb.se/contentassets/9fea3d70e4504ca4aee5d1f83617f995/raminstruktion-for-det-svenska-civila-beredskapsarbetet-inom-ramen-for-Nato-pff.pdf.

122. Ju2021/00361 Raminstruktion för det svenska civila beredskapsarbetet inom ramen för Nato/PFF, https://www.msb.se/contentassets/9fea3d70e4504ca4aee5d1f83617f995/raminstruktion-for-det-svenska-civila-beredskapsarbetet-inom-ramen-for-Nato-pff.pdf.

Lesson 2: Systematic information and cyber security work makes a big difference

Organisations that conduct systematic information and cyber security work, and have working methods to identify risks and do not leave risks without action, will be better equipped in case of heightened alert or war. How a "cyber war" develops during a war situation is largely determined long before an outbreak of war, by how well the organisations work systematically and preventively with information and cyber security.

We previously presented how Ukraine intensified its cooperation on information and cyber security issues following the cyber-attack against the Ukrainian energy companies in 2015, and that Ukraine adopted a cyber security strategy in January 2016 and set up a national cyber security coordination centre. The centre's importance to the resilience of Ukrainian society gradually grew and its mandate was further expanded in 2019, for example regarding cooperation developed with NATO, the EU and the United States. Ukrainian government representatives assess that the support received by the country has been crucial to its ability to defend itself against Russian cyber-attacks.

Organisations working on information and cyber security in a systemic way will:

- Know what information systems and what information they need to protect, and in what ways.
- Possess a deeper knowledge of the risks they face, and of how these may change if the risk of war arises.
- Work with risk prevention to an extent that they deem appropriate.
- Manage an ability to handle incidents.

The large amount and variety of cyber-attacks used against Ukraine demonstrates the importance of maintaining a high quality in the systematic information and cyber security work. As cyber-attacks pose a constant threat to every part of society, it is crucial that society as a whole maintains a common preparedness related to the risks that may arise. Ukraine's defence demonstrates, through its own efforts and cooperation with various sympathisers, how it is possible to strengthen the ability to work to prevent consequences and to deal with incidents that occur.

The results of the The Infosec Checkup, which was carried out in 2021, pointed out serious shortcomings in large parts of the systematic information security efforts in Swedish public administration. It therefore seems likely that Sweden is currently not as well equipped as, for example, Ukraine was at the time of Russia's invasion in February 2022.

Digital supply chains maintain essential societal functions

Organisations' IT environments are constantly changing and thus there is a dependence on the uninterrupted delivery of goods and services. Attacks on the energy supply and electronic communications could mean that information systems cannot be used. Components are needed to establish, maintain, develop and restore information systems. Mono-dependencies make societies particularly vulnerable.

In 2021, as we reported above, there were a large number of intrusion attempts against Ukrainian public administration as well as against defence companies, humanitarian organisations and suppliers in digital supply chains of particular importance for Ukraine. During the first day of the full-scale invasion, Viasat's satellite-based KA-SAT network suffered an extensive outage. The outage was caused by a supply chain attack in which an update of firmware, which contained malware, was distributed to and installed in the special modems used to connect to the network.

The malware Industroyer2 discovered on April 12 2022 is an example of attacks on the energy supply that, if successful, can leave essential societal functions and millions of residents without power.

This type of attack on, for example, the energy supply and electronic communications shows how complex dependency chains make societies vulnerable. Alternative solutions are necessary to ensure that essential societal functions continue to work even when information systems and processes are attacked.

Robustness and redundancy make a society resilient

The basis of a resilient society is that functions and organisations providing essential services are equipped to withstand factors that could lead to incidents. It is also crucial that there are alternative operators who can provide similar solutions so that an operation can continue even if an individual supplier is affected by an incident. In the event of incidents from which it is not possible to recover quickly, several available solutions are particularly important. From an information and cyber security perspective, this means that organisations protect their information, their information systems and their services.

Robustness is achieved by the organisation, together with its subcontractors, carrying out systematic risk prevention and risk management work, with low risk tolerance. The incident reporting, and the result of the latest measurement in the work with the The Infosec Checkup, indicate that it is common in Sweden that there is a lack of systematic work with regard to the robustness of the organisation. Ukraine has shown examples of good robustness; for example, the mobile network has continued to function despite extensive physical and digital attacks.

Redundancy is achieved, in some areas, by having a functioning market where organisations can compete and where there is the possibility for more than one organisation to provide the same kind of service. In other areas, such as healthcare, other measures may be required. At present, in some areas in Sweden, there is the opposite of redundancy. In e-authentication, for example, many organisations have a mono-dependence on a particular service. Since many organisations have a mono-dependence on the same service, several operations

may be affected if that service no longer functions properly. The war in Ukraine shows the importance of redundancy, such as when SpaceX assisted the country with access to Starlink terminals that could replace the attacked Viasat network.

Today's Swedish society is completely dependent on a continuous supply of goods and services. An attacker can take advantage of this and knock out or disrupt critical parts of a supply chain necessary for society to function normally. All measures normally taken to strengthen Swedish capabilities in the cyber area will also strengthen resilience in a war situation.

→ Recommendations

- ✓ Systematic information and cyber security work must be prioritised and resourced.
- ✓ Conduct regular follow-up, such as through The Infosec Checkup, in order to increase the robustness of information management.
- ✓ Every essential societal function needs to map its supply chains and carry out vulnerability analyses involving both suppliers and subcontractors.
- ✓ All actors working in support should examine how they can intensify the already ongoing work to support those actors in both the public and private sectors who have problems implementing the necessary measures

Lesson 3: Apply the all-hazards approach

Cyber-attacks often receive a lot of attention, especially in comparison to other IT incidents. It is perhaps more exciting to investigate and read about malicious intent and actors than that a system administrator failed with an update. It's a better and more exciting narrative.

The truth, in any case, based on the overall picture of reported IT incidents presented in the chapter Reported IT incidents in 2022, is that the normal picture is similar to previous years. The most common causes continue to be mistakes (often in connection with the implementation of changes in the IT environment) and system errors (which could often have been avoided through changes in the IT environment). In fact, the number of reported attacks actually dropped slightly in 2022 compared to 2021. Furthermore, it is notable that about half of the reported attempted attacks were fairly unsophisticated denial-of-service and phishing attempts, which are relatively easily remedied with good practices and trained personnel.

In this report, MSB proceeds from the IT incidents reported to the agency. There are unreported figures. There are actors who are required to report incidents, but who do not make reports. There may be many reasons for this, and it is also possible that the willingness to report has been further hampered by the fact that organisations do not want their incident report to be automatically converted into a police report, in accordance with what was described in the chapter "Important news in 2022". It should also be kept in mind that there are actors not required to make reports who are under attack and that this affects the picture of the number of attacks.

The normal picture remains that a large number of the incidents that occur every year are caused by mistakes and system errors. The normal picture also includes that a number of serious incidents are caused by mistakes or system errors every year. This reaffirms the importance of the all-hazards approach for maintaining essential societal functions and essential services.

However, the above reasoning does not imply that the risk of cyber-attacks should be underestimated. Especially in connection with the serious world situation. The fact that websites belonging to the Finnish Parliament[123] and Norway's BankID[124] were attacked indicates the desire and capacity to cause societal harm. It is therefore important to take into account the lessons outlined in this chapter in the short- and long-term work on systematic information and cyber security.

The Ukrainian IT army and the Belarusian cyber partisans are examples of sympathising hacker groupings with the aim of carrying out counterattacks, causing some cyber security experts to express concern about the actions of the hacktivists. For example, the Czech cyber security organisation Avast Software highlighted that the execution of denial-of-service attacks is illegal regardless of the target of attack and calls on everyone to refrain from engaging in such initiatives, regardless of which side they sympathise with.[125]

Attack strategies from the war in Ukraine that a Swedish cyber defence needs to be able to meet

To understand what a cyber defence may face in the future, it is valuable to study the attack strategies used in a modern war like that in Ukraine. It was discussed earlier in this report that Russia has had different cyber strategies at different stages of the war. Following the initial phase of the full-scale invasion, methods deemed to be more sophisticated were used, such as the Viasat attack. The period thereafter was more primitive where the cyber strategy consisted primarily of denial-of-service attacks and intrusion attempts through phishing.[126] Some lessons that can be learned about cyber warfare that a cyber defence needs to be able to meet are that:

- A planned physical attack is likely to be preceded by a lot of intrusion attempts aimed at establishing opportunities to execute malware in order to lower the defence capability and resilience at the start of the physical attack.
- As those intrusions are used and malware is executed, respectively as those intrusions are detected and averted, the attacker will gradually ”use up” his most destructive cyber weapons, just like missiles and artillery are used up.

123. Urwäder, Jasmine. Riksdagens webbplats utsattes för rysk hackerattack – en av de mest kända hackergrupperna under kriget I Ukraina, sager expert. Svenska Yle. 2022-08-09, https://svenska.yle.fi/a/7-10019443 (downloaded 11/2022).

124. TT. Ryska hackare: Attack var hämnd för norsk blockad. Dagens Industri. 2022-06-29, https://www.di.se/nyheter/ryska-hackare-attack-var-hamnd-for-norsk-blockad/ (downloaded 11/2022).

125. Streda, Adolf & Kaloc, Jakub. *DDoS hacktivism: A highly risky exercise*. Avast, 2022, https://blog.avast.com/ddos-hacktivism-avast (downloaded 12/2022).

126. Beecroft, Nick. *Evaluating the International Support to Ukrainian Cyber Defense*. Carnegie Endowment for International Peace. 2022-11-03, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (downloaded 11/2022).

- Once the advanced cyber weapons are used, the assault image will increasingly be dominated by more primitive attacks (such as denial-of-service attacks) and new attempts at intrusion.
- The less preparation an attack requires, the more it will be used.

Cyber-attacks can be carried out for a broad range of purposes, for example, they may aim to:

- Cause harm to the party under attack (such as destroying important information assets or spreading fear).
- Prevent utility to the party being attacked (such as disrupting essential services or interrupting industrial production).
- Provide utility to the attacker (espionage).
- Prevent harm to the attacker (disrupting defence systems, or command and control).

When cyber-attacks do not produce the desired effect, the next step can be physical attacks

Prior to the full-scale invasion of Ukraine in February 2022, different types of cyber capabilities were used and during the war, conventional warfare has been used in parallel with cyber warfare.[127] Above all, before, but also after the full-scale invasion, Ukraine has been subjected to a large amount of cyber-attacks. Although there are unreported figures, most analysts conclude that the results of these attacks have been somewhat limited. Apart from the written-about wiper attack on the Viasat K-SAT network in February 2022 and another couple attacks targeting Ukrainian authorities that were successful from a Russian point of view, even including those during the first phase of the invasion, there have been unexpectedly few and small disruptions to Ukraine's infrastructure reported as a result of cyber activities.

One of the few examples of an attack where it was clear that cyber-attacks were coordinated with attacks with conventional weapons is when Ukrainian media companies suffered a cyber-attack while a television tower in Kiev was fired on with missiles in March 2022. What can be clearly observed is an increase in conventional weapons attacks on Ukrainian civil infrastructure. A huge amount of missiles and drones fired from aircraft, ships and the ground have been used to take out both electricity and water supply, as well as hospitals and railways. According to Ukrainian Defence Minister Reznikov, approximately 3,000 missiles have been fired at Ukraine up to mid-November 2022.[128]

127. Burt, Tom. *The hybrid war in Ukraine*. Microsoft, 2022, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/ (downloaded 11/2022).

128. Reznikov, Olekseii. Four enemies of the russian missile arsenal: brilliant Ukrainian air defense forces; inept russian missile forces; sanctions; time. Twitter 2022-11-22, https://twitter.com/oleksiireznikov/status/1594998365170896896?s=20&t=8odifazCOZgwPMN8dFTQlQ (downloaded 11/2022).

Since advanced missiles are incomparably far more expensive than cyber-attacks, it is easy to assume that the increasing use of them is due to the fact that cyber-attacks have not produced the desired results.

→ Recommendations

- ✓ Shift work on dimensioned threat scenarios into high gear and include sophisticated cyber-attacks before the start of the war.
- ✓ Strengthen the ability to search networks and computers after dormant malware, and create procedures to actually do this regularly.
- ✓ Create a strategy for how Sweden should relate to sympathetic hacker groups in heightened alert or war.

Lesson 4: Good resilience is crucial in hybrid warfare

Experience from Ukraine shows that in the event of an increased risk of war, the volume of antagonistic cyber activity is highly likely to increase significantly. The problems of non-antagonistic IT incidents (system errors and mistakes) will also persist in a situation of heightened alert or war, with the probable difference that more incidents, including serious incidents, will occur. Two factors suggest this:

- The circumstances under which work and changes in the IT environment are carried out are likely to be more stressful;
- Some organisations may have a shortage of staff to implement changes in the IT environment. International personnel may leave the country, citizens of the country may be called upon by national defence and, at worst, personnel may have been injured or killed.

In such a situation, the choice consists of either making changes with an increased risk of mistakes, or of refraining from making changes, which may make the system more vulnerable than it would have been had it been updated according to plan[129].

Digital supply chains are an important area and it can be noted that it is of great importance to work out mono-dependencies to individual products and services; especially, if there are several essential societal organisations that depend on the same product or service. In a situation of an increased risk of war, the complexity of the loyalty of the suppliers also comes into question. If there is reason to believe that such a supplier has a dependence on the foreign power to which the conflict relates, that supplier must be quickly excluded from the supply chain.

129. The report “Changes that both threaten and protect” raises this problem and makes recommendations for more secure changes to our information systems. Stockholm: MSB, 2022. https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/.

Societal impact of the use of cyber means

In advanced economies of a certain size, such as Sweden, specific kinds of essential services are provided by multiple organisations often in competition with each other. This means, for example, that an outage at a bank does not make it completely impossible to make payments, but rather payments can be handled with the support of other banks in such a situation. For payments not to be possible to make at all, a number of organisations must be unable to provide their services at the same time. It is especially in such situations that it can be said that incidents have serious societal consequences.

Three kinds of risks related to the information and cyber security area that may result in such an effect, are when:

- Things that are not to be delivered, in a digital supply chain, are still delivered to many organisations at the same time whereby threats or obstacles arise in them.
- Things that are to be delivered, in a digital supply chain, are not delivered to many organisations at the same time and there are no alternatives to what would be delivered.
- Many organisations have the same or similar Internet-exposed infrastructure for incidents (vulnerability).

Resilience enables a society to recover quickly

In addition to robustness and redundancy, resilience is crucial to create a strong society. Once an incident has occurred, a rapid recovery is important.

Resilience is achieved by the organisation, together with its subcontractors if necessary, planning and practising both incident management and continuity management. It is also important to have established communication channels to its suppliers before an incident occurs. During the war in Ukraine, resilience has been strengthened through, among other things, cooperation with sympathisers from the rest of the world to increase the possibility of recovery after an incident. For example, several large companies have allowed space in their cloud services for the Ukrainian state and Ukrainian organisations to back up their information.

Component shortages and procurement in difficult times

Having access to spare parts, components, in order to quickly restore defective hardware is central to good resilience. Component shortages can occur for various reasons, from a fire in a single central factory, to stress tests of the entire system, such as during the COVID-19 pandemic. Even in good times, delivery times for specific components can be many months long. The fact that essential societal functions are prepared for incidents or crises through good stockpiling of especially crucial components cannot therefore be emphasised enough.

It is also important that this is taken into account in procurements and is linked to quality requirements. Key actors in a sector should take into account the establishment of contacts in order to make a joint procurement. Instead of competing with each other in a shortage situation, a joint procurement proce-

dure, and thereby a larger order, may instead increase the probability that the order is prioritised by the supplier. This is all the more important as a relatively small country like Sweden is at risk of being downprioritised for larger clients.

→ Recommendations

- ✓ In the event of heightened alert or war, access to information and authorisation must be restricted for personnel and subcontractors who can be presumed to have loyalties other than to Sweden.
- ✓ Plan and practice incident and continuity management.
- ✓ To avoid a shortage situation in operations, ensure access to particularly important components.
- ✓ Prepare to be able to activate a joint procurement procedure.

Lesson 5: Legal barriers hamper the cyber defense

As a result of the changing security situation in a large-scale war in Europe, as mentioned above, the robustness, resilience and redundancy of essential societal functions in terms of information and cyber security need to be strengthened, especially when it comes to supply chains. This will enable essential services to maintain and secure the most essential societal functions, and contribute to the capabilities of total defence, in the event of severe stress or under heightened alert and war. To achieve this, stakeholders need support. Sweden's conditions for coping with both normal situations (peacetime) and crisis and war are much better if the conditions mentioned in the above lessons are achieved.

However, ongoing work and the basis for this report show that several measures that could contribute to the strengthening of the civilian arm of cyber defence require new or changed legal regulation in order to effectively meet current and future needs in the field of information and cyber security. MSB believes that in many cases increased resources are not enough, but that legal reinforcement is also needed to ensure that:

- Society's demands for actors who conduct activities of importance to the functioning of society and total defence cover all relevant actors, are clear and are complied with.
- The government agencies that support these actors can use appropriate tools adapted to today's and tomorrow's technologies.
- Sweden's digital sovereignty can be secured.

Actor level

Set requirements on essential societal functions

Digitalisation presents us with major opportunities, but also risks. An increasing proportion of all activities in society depend on networks and information systems. This is why information and cyber security is an issue that concerns all of society today.

The need for security is particularly important in terms of essential services, which must work in all circumstances in order to maintain the essential societal functions. To achieve this, society needs to make appropriate demands of all private and public actors currently operating essential services and provide support for this work. To ensure robustness, resilience and redundancy in practice, society needs to better inform itself about IT incidents, monitor compliance with the requirements and continuously develop requirements and support to meet new challenges and opportunities in the field.

The current regulatory framework does not provide sufficient opportunities for this. Today, far from all key actors in society are subject to explicit requirements to conduct systematic information and cyber security work for all of their information in the essential services. The requirements apply only to certain types of information or to certain types of activities carried out by the organisation, which creates a not entirely contiguous "patchwork quilt" of requirements to relate to.[130] The same applies to implementing appointed security measures and reporting IT incidents.[131],[132] Although the requirements for incident reporting and systematic information security work are similar for those covered, the requirements for implementing specifically appointed security measures in their information systems are partly different. Different supervisory agencies in NIS impose different requirements on NIS suppliers in their sectors. This is despite the fact that the security measures that organisations need to implement to achieve a basic level of information security in essential services are largely similar. Another difference in today's requirements concerns supervision. Certain requirements, those imposed under the NIS regulations, are subject to supervision, while the requirements imposed on government agencies in accordance with the Ordinance on Central Government Agencies' Preparedness are not. At the same time, The Infosec Checkup shows serious deficiencies in the information security work in Swedish public administration. Only a small minority of government agencies are able to meet the requirements in MSB's regulations even though they have been in place since 2009. This demonstrates the importance of combining requirements with follow-up. In the appropriation letters to some government agencies for 2023, the Government has requested that they report their information security work. This makes an important contribution to the follow-up work but is not considered to be sufficient to deal with identified shortcomings. Far from everyone receives such appropriation letter assignments and different ministries also request different information which makes it difficult to ensure compliance with the rules. The assessment is that this cannot replace a supervisory procedure.

130. The NIS regulations only apply to information security in the essential or digital services provided by the provider. The data protection regulations protect personal data and the protective security regulations target information that requires protection on the basis of Sweden's national security. Only government agencies are required to conduct systematic information security work for their entire operation.

131. In short, it concerns the group of actors covered by the NIS regulations, providers of essential or digital services, as well as government agencies.

132. The sectors are energy, transport, banking, financial market infrastructure, healthcare, supply and distribution of drinking water and digital infrastructure. In addition, suppliers are covered by certain specific digital services.

At the time this report is being written, work will begin on the Swedish implementation of the so-called NIS 2 Directive[133], which will replace the existing NIS regulations. The aim of the new directive is to further reduce the fragmentation of the EU's internal market by stipulating minimum rules for a coordinated regulatory framework. Depending on how the directive is implemented, there is potential to contribute to reducing fragmentation nationally as well. The scope of the rules is extended to cover actors in more sectors than the existing NIS Directive.[134] Although the scope is extended, it will not be comprehensive. For example, it is not necessary to include municipalities. However, the NIS 2 Directive emphasises that Member States should endeavour to ensure that even essential societal functions excluded from the scope of this Directive achieve a high level of cyber security.[135] This is because cyber threats are intensifying and becoming increasingly sophisticated.

Securing digital supply chains already now

What security requirements are placed on essential societal functions is also central. One area where the need to review safety has grown sharply is digital supply chains. When IT incidents with a major impact on society occur, it is often due to a problem in a supply chain. They are at their worst when the disabled operator provides a specific service for which an organisation cannot, for various reasons, be expected to have redundancy, also known as a mono-dependency. An often-cited example of this in recent years is when Kaseya was subjected to a ransomware attack and several Swedish retail companies lost access to their cash registers. MSB's report "Digital supply chains under threat: 50 recommendations to strengthen societal security"[136] advocates the importance of regulating mono-dependencies. Furthermore, the report highlights that specialisation is increasing year on year and that it is therefore likely that more and more organisations will be exposed to mono-dependencies without knowing it.

The NIS 2 Directive draws attention to the need to increase the security of digital supply chains, and requirements are not only set on those who operate essential services, but also on government agencies that coordinate the NIS work as well as on EU institutions. This is positive and is deemed to contribute to increased security. However, the new NIS regulations will not enter into force until October 2024, while the work to strengthen the security of supply chains needs to begin now, preferably as part of the work on civil defence. Furthermore, the analysis of supply chains needs to be done on aggregated data, as it is only then that the mono-dependencies of several operations on the same service become apparent.

With the new preparedness system put in place on 1 October 2022, preparedness sectors were established for the ten most central societal functions. The mapping of mono-dependencies in these sectors, the identification of vulnera-

133. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

134. The sectors added are wastewater; management of ICT services; public administration; space; postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital suppliers and research.

135. The NIS 2 Directive, reasons (13).

136. Digital supply chains under threat: 50 recommendations to strengthen societal security https://rib.msb.se/filer/pdf/29829.pdf.

bilities and the development of proposals on how to deal with them are urgent. Such work provides an excellent basis for and a head start in the continued work on supply chains within the framework of NIS 2. In this context, society would need to do a concerted job in which the involvement of private actors is central.

Facilitate IT incident reporting by stakeholders

A great source of knowledge on the number of IT incidents, as well as their cause and effect are the reported IT incidents that MSB continuously receives[137]. The supporting evidence is, however, not comprehensive. On the one hand, not all essential societal functions are subject to the requirement to report IT incidents and, on the other hand, MSB makes the assessment that not all IT incidents subject to required reporting are actually reported. All in all, this means that there is a large number of unreported IT incidents that take place in essential societal functions.

Here, too, the NIS 2 Directive will be able to contribute to improvements by extending the IT incident reporting requirements to more sectors. Due to the threat to Sweden, it is essential to ensure that all essential societal functions are covered when the NIS 2 Directive is implemented in Sweden. Maintaining an overall picture of the IT incidents is a prerequisite for MSB to be able to fulfil the mission of rapidly reducing the risks and consequences of IT incidents, which ultimately strengthens society's robustness.

In terms of the second challenge due to underreporting, several aspect may play a role. It may be a matter of a lack of knowledge, but also uncertainty about the possibilities that exist to keep information about a reported IT incident confidential.

In public record request cases, MSB classifies as secret who has been affected, what happened, and other information that may facilitate an attacker's use of the information in an attack. The agency has received support for this interpretation in the Gothenburg Court of Appeal,[138] while the Swedish Food Agency has been given partly different feedback from the Stockholm Court of Appeal where the information on whether or not a report was submitted to MSB was deemed to be covered by secrecy. The differences in the rulings of the judges are unfortunate because the basis for MSB's not disclosing information about whether a report was received or not is also becoming relevant at the reporting actor for the corresponding information. Another challenge is that secrecy applies only to information about "security and surveillance measures" not all information provided in an IT incident report although it may be perceived as sensitive by the victim for other reasons, such as technical descriptions that do not have direct bearing on security measures but are relevant to the understanding of the event and its consequences. In order to support stakeholders with in-depth technical analyses and to increase the security of reporting actors and their confidence that submitted IT incident reports are guaranteed protection, there is a need not only to clarify but also to extend the secrecy regulation.

137. Incident reporting takes place in accordance with Section 14 of the Ordinance (2022:524) on Central Government Agencies Preparedness and Sections 18 and 19 of the Act (2018:1174) on Information Security for Essential and Digital Services.

138. Case no. 2144-21.

Support from government agencies

Simplify collaboration and co-creation

The importance of collaboration is best explained in Lesson 1, but within the framework of Lesson 5, the legal aspect of collaboration and co-creation is in focus. The possibilities to build more effective support in IT incidents through in-depth collaboration were, for example, one of the reasons for the establishment of NCSC-SE. IT incident management is just one example of areas where technical and security developments create a need for collaboration between government agencies that goes beyond traditional forms of cooperation.

When government agencies cooperate, information quickly goes beyond the authority's boundaries, whereupon it becomes an official document. If several agencies work in a joint workspace that is available to external actors, all actors must prepare for the information they work with there being considered to be an official document regardless of the stage the work is in. In a public record request case, the information may not need to be disclosed, but co-creation is difficult without set conditions. An authority's working document is not subject to the principle of public availability to official documents in order to allow the authority to work in peace and not to risk the disclosure of half-finished proposals. The same needs arise in this type of cooperation and co-creation. Cooperation and co-creation provides improved efficiency and better quality, so the promotion of co-creation should be made possible. Since the formulation of the principle of public availability to official documents is laid down in the Constitution, an alternative option may be to review the possibility of introducing secrecy for co-created data that are at the same stage of development as working materials.

Digital sovereignty

Stronger control over IT resources

Digital sovereignty can have several dimensions, but one key element is for a country to have control over its essential IT resources. This is not the case in Sweden today. Most of the tools used both privately and professionally are provided by foreign, often American, companies. Strengthening the access to and control over fundamental societal information and information-bearing infrastructure, as well as digital supply chains during crises and heightened alert, and thereby strengthening digital resilience, is an important component of total defence.

In order to build digital sovereignty that strengthens Sweden, a number of issues need to be investigated, not least the legal issues of control, in what way and over what? How should digital sovereignty relate to the EU and should certain essential societal functions have to use certain types of digital infrastructure? The issue can be favourably addressed within the framework of the work to produce future defence decisions.

Data storage facilities

The success of Ukraine's cyber defence can be attributed in part to the established international cooperation which enabled rapid action to protect Ukraine from attacks and to prevent and mitigate the damage that still occurred. An example of preventive work was that Ukraine chose to copy virtually the entire

data content from its authorities' IT systems and many of its government servers to international cloud services. Both of these measures contributed strongly to the resilience of Ukraine's critical IT systems. But such measures would be illegal in Sweden today.

Sweden currently has no coordinated preparedness in terms of handling and evacuating critical societal data in the event of serious incidents such as natural disasters, wars or cyber breakdowns on a larger scale. In order to ensure that important information is not lost and to ensure that data is kept confidential, it is important to build up such preparedness systematically and strategically.

A development of its own cloud-like solutions where Sweden can retain control and the exclusive rights to its data may be a way to go. These could be appropriately used even in times when critical data does not need to be evacuated, for example to secure the operation of essential societal functions. Customising a solution for Sweden requires innovation as well as resources, but also a number of legal considerations, ranging from competition issues to protective security. Therefore, an investigation into Sweden's digital sovereignty needs to be carried out.

→ Recommendations

- ✓ Ensure that all essential societal functions are subject to collective information security requirements by extending the scope of the upcoming NIS 2 regulations.
- ✓ Combat fragmentation by as far as possible setting the same basic requirements on information and cyber security in essential societal functions.
- ✓ Instruct MSB, together with sector-responsible agencies, to identify mono-dependencies in the new preparedness areas, and make proposals on how identified mono-dependencies should be managed.
- ✓ Clarify and extend the protection of IT incident reports under the Public Access to Information and Secrecy Act.
- ✓ Improve the conditions for government agencies to cooperate through co-creation, possibly through secrecy for joint working materials.
- ✓ Appoint an investigation into Sweden's digital sovereignty.
- ✓ Appoint an investigation into how Sweden can prepare to back up critical societal data.

Conclusions

Conclusions

The full-scale invasion of Ukraine left the European security architecture in pieces. Sweden has applied for membership in NATO and is contributing with military equipment to a country at war. In the new cyber landscape, the map of needs has been redrawn. In order to ensure the functioning of essential services under the risk of war and in war, Swedish information and cyber security must be given higher priority and allocated more resources. The necessary measures need to be implemented and evaluated.

The cyber-attacks used during the war in Ukraine have been of a different nature, with the aim of achieving different objectives. These objectives can be divided into four categories:

- obstructing utility in Ukrainian society
- causing harm in Ukrainian society
- preventing harm to the attacker or attacker's client
- causing utility to the attacker or attacker's client.

On its own and with extensive help from other countries and volunteers, Ukraine has had to deal with cyber-attacks for many years both before the large-scale invasion and since. This report has presented how this has improved the country's cyber defence capability and that many cyber-attacks were therefore able to be averted. The impact of cyber-attacks has thereby been less than expected.

From the cyber warfare in the war in Ukraine, it is possible to see how different factors can play a crucial role in defence on the cyber front. In order to face a scenario of an increased number of sophisticated cyber-attacks before a war, the minimum level needs to be raised. At the same time, the reported incidents from 2022 show that most incidents are due to system errors and mistakes. Therefore, it is crucial that essential societal functions conduct work based on the all-hazards approach. To succeed, systematic information and cyber security efforts must be prioritised and given resources.

Sweden's minimum level must be raised and the lessons from Ukraine show that, in order for a country to be resilient, this work must begin several years before a full-scale outbreak of war. In addition, regular follow-up, for example through the implementation of The Infosec Checkup, is needed to increase

resilience in general, and especially for essential societal functions. All actors working in support need to intensify the work to those essential societal functions that have problems implementing the necessary measures.

Every essential societal function needs to map its supply chains and carry out vulnerability analyses covering both suppliers and subcontractors. Furthermore, these actors, either themselves or through a partner, must ensure the ability to search networks and computers for dormant malware and create procedures to do so on a regular basis. In case of heightened alert or war, information assets and authorisations must be restricted for personnel and subcontractors who can be presumed to have loyalties other than to Sweden. In addition, incident and continuity management must be planned and trained. The supply of particularly important components must also be secured. To this end, preparations to be able to activate a common procurement procedure are recommended.

The cyber war in Ukraine shows perhaps most of all the importance of cooperation. Sweden needs to further strengthen the cooperation in the field of cyber security both nationally and internationally, and create procedures to share intelligence information with international partners. Procedures for how international assistance can be received are also needed. In addition, planning is needed for states of readiness in organisations responsible for essential societal functions. Sweden also needs a strategy for how it should relate to sympathetic hacker groups and their actions in case of heightened alert or war.

In order to respond fully to the lessons learned from the report, it is necessary to ensure that all essential societal functions are subject to collective information and cyber security requirements. Linked to this, fragmentation needs to be countered as far as possible by setting the same basic requirements on information and cyber security in essential societal functions. MSB wishes to be tasked, together with sector-responsible government agencies, to identify mono-dependencies in the new preparedness areas, and make proposals on how to manage identified mono-dependencies.

In addition, the Public Access to Information and Secrecy Act's protection of IT incident reports needs to be clarified and extended, and it should be considered whether sanctions should be imposed on those organisations that do not comply with their reporting obligations. Government agencies also need to be given better conditions to cooperate through co-creation.

One investigation should be appointed to look into how Sweden can prepare for backing up critical societal data, and another investigation should be appointed to further explore Sweden's digital sovereignty. It should also be considered whether an actor shall be granted supervisory capability in the field of information and cyber security.

Future outlook

Future outlook

If 2022 was the year when large-scale war came close, 2023 looks to be a year characterised by partnership. In the first half of 2023, Sweden is the President of the EU, and the membership application to NATO means enhanced cooperation on the introduction of new processes and procedures for information sharing and co-creation.

In recent years, society has faced major challenges. The COVID-19 pandemic increased the rate of digitalisation and widened the already high-profile gap between digitalisation and information and cyber security. As a result of the war in Ukraine, the importance of a resilient cyber defence has been prioritised and new needs linked to information and cyber security have emerged. This report shows how broad international cooperation has been a key to strengthening Ukrainian cyber defence.

The results from The Infosec Checkup, which were reported to the Government in 2022, revealed serious deficiencies in the systematic information security of Swedish public administration. 80 % of organisations were unable to live up to the lowest level of the model. However, MSB saw that as many as a third of all organisations could climb up by the next measurement with relatively limited improvements. This is why MSB confidently looks forward to cooperating with public administrative bodies when the next follow-up with The Infosec Checkup will be carried out in 2023.

The attack trends that received media attention in 2022 are also likely to continue as long as the countries of the world do not join forces to significantly change the incentives. MSB will continue to follow the trend and as mentioned in last year's report, a connected world affects all of us. The negative consequences in the shadow of the benefits of digitalisation mean that MSB hopes for an increased willingness from more organisations to report IT incidents in 2023.

In the spring of 2023, Sweden holds the EU Presidency. A number of meetings will be held in Sweden and EU issues will be prioritised. Sweden's cooperation with other EU Member States contributes to strengthening Swedish information and cyber security. Some of the most central collaborations are exemplified by the NIS Cooperation Group, the CSIRT network and EU-CyCLONe. Co-operation at the policy level also strengthens common information and cyber security. Especially key examples are the EU's cyber defence policy, the Cyber Resilience Act and the AI Regulation.

Never before has a membership application to the NATO Defence Alliance been handled as quickly as the Swedish and Finnish application. 28 out of 30 Member States ratified Swedish membership in 2022. Full membership is expected to strengthen the political community and cyber security cooperation. Today, Sweden is indeed already cooperating with NATO in the framework of the Partnership for Peace. The starting point for this cooperation is a strengthened emergency preparedness. This is being done in areas such as the food and energy supply, and safe transport. During 2023, Sweden will pursue the aim of Swedish participation with a focus on civilian preparedness work. Sweden seeks an increased presence in all relevant NATO structures for strengthened political dialogue and information exchange. MSB will continue to maintain an overall picture of Swedish participation in this work and pursue civil defence issues.

In a connected world, information and cyber security affects all of us. Together, we take responsibility.

Swedish Civil
Contingencies
Agency

651 81 Karlstad Tel +46 (0)771-240 240 **www.msb.se**
Publ.nr MSB2208 – June 2023 ISBN 978-91-7927-402-3