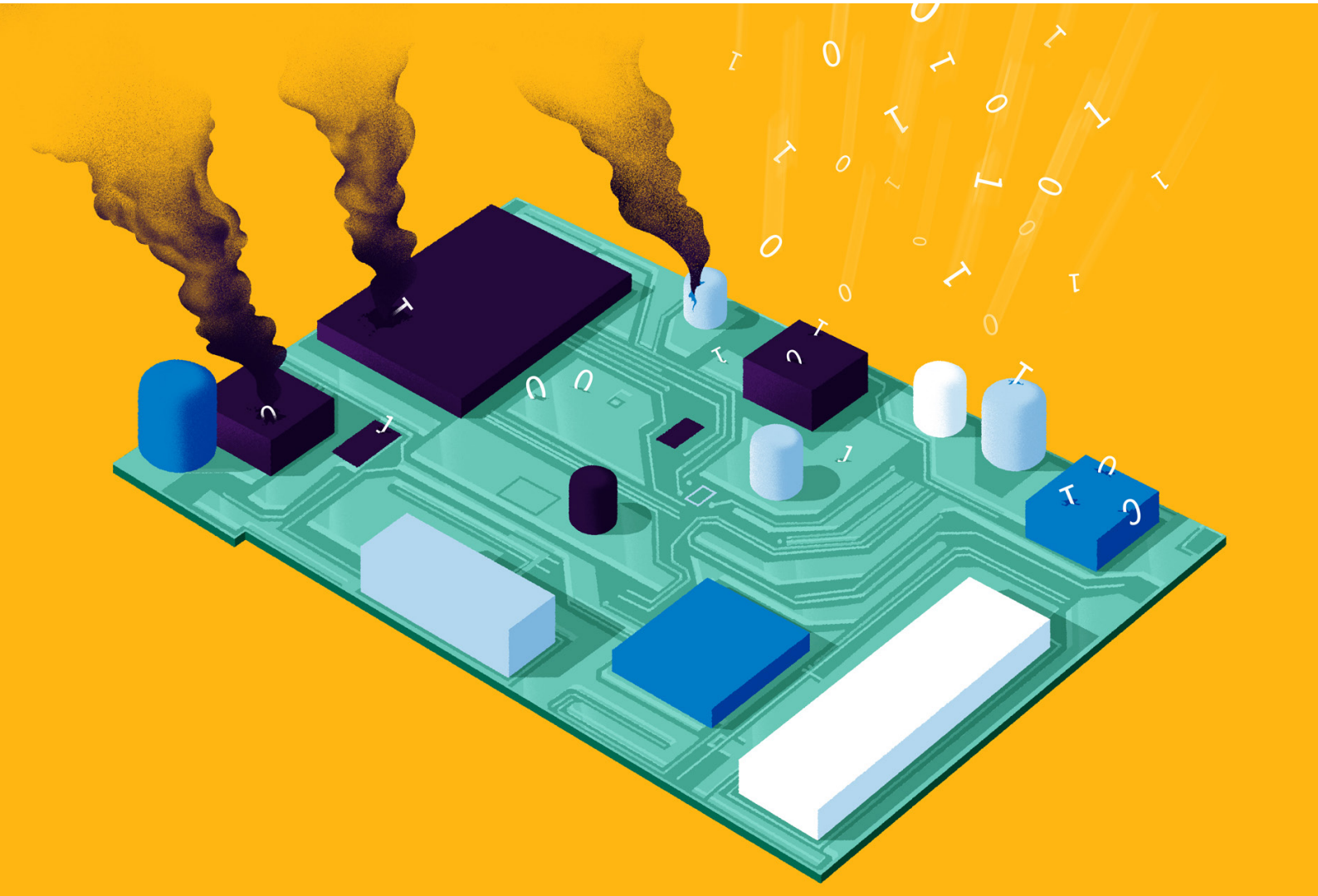
National Cyber Security Centre
Ministry of Justice and Security

Four cyber security lessons from one year of war in Ukraine



Participating organisations

This product is published by the National Cyber Security Centre (NCSC), the Digital Trust Center (DTC) and the Computer Security Incident Response Team for Digital Service Providers (CSIRT-DSP) and is the outcome of a knowledge-sharing session with cyber security experts from various Dutch government bodies.

Cyber security experts from the NCSC-NL, the DTC, the CSIRT-DSP, the Ministry of Foreign Affairs, the Netherlands Defence Academy (NLDA), the General Intelligence and Security Service (AIVD), the Defense Intelligence and Security Service (MIVD), the National Coordinator for Counterterrorism and Security (NCTV) and the Defence Cyber Command took part in the session.

Contents

Foreword

A year ago, Russian troops crossed Ukraine's national borders, thus bringing war back onto European soil. The course that the invasion has taken is well known. The rapid conquest that Russia envisaged has turned into a bloody conflict that has claimed tens of thousands of lives and is still ongoing. As a result of the war – invisible to the naked eye – there has also been fighting in the digital sphere by pro-Russian and pro-Ukrainian actors.

The NCSC has been monitoring this digital conflict closely and with maximum vigilance since the start of the war. Together with our national and international partners, we detect and analyse cyber threats 24/7 that could be related to the conflict in Ukraine and offer action strategies to companies and organisations in the Netherlands. Fortunately, the impact of cyber attacks in the Netherlands has hitherto been limited, but that could change. Vigilance remains essential.

What can we learn from the past year? As with all major events, it is important to take a retrospective look from time to time. We can learn from that and thus look ahead again. This is why the NCSC took the initiative in December to review the past year's experience with our partners. What kind of cyber attacks did we see, how did they work, and what kind of actors were behind them? Another important point: what measures can we take to combat them?

This report gives a concise description of the four main cyber security lessons from a year of war in Ukraine. These lessons learned provide us with valuable insights which help us to be prepared for future cyber attacks. The more knowledge we gain of our own actions and malicious actors in the digital sphere, the more we can improve the Netherlands' digital resilience.

The war in Ukraine has had a major impact in the Netherlands as regards raising awareness. We are seeing a growing realisation on the part of organisations and companies of our economic reliance on digital services and their vulnerability. As a result, the private and public sectors are beating a path to each other's doors and exchanging information. More stringent new European cyber security legislation will encourage this trend still further.

As the war in Ukraine enters upon a new phase, it is important for organisations and companies to maintain their joint efforts in the area of cyber security. That starts with more robust, more secure IT environments. The NCSC-NL will continue to strive to improve communications between all concerned and share threat information and action strategies promptly.

Together we need to be on the lookout for cyber attacks, for things that happen just when you are not expecting them. We can only minimise the impact of such attacks on the Netherlands and the world by working together.

Hans de Vries
Director NCSC-NL

The main lessons

In this report, the NCSC-NL, along with the DTC and CSIRT-DSP, looks back on a year of war in Ukraine and the cyber security lessons that can be drawn. We consider not only the digital threats but also measures to increase digital resilience in partnership with cyber security partners in the Dutch government. This chapter provides an introduction, outlining the context of and run-up to the report as a whole.

Digital attacks related to the war have not hitherto caused any major disruption in the Netherlands. The attacks that have been carried out have had only temporary, local effects, hence the impact has been limited.[1] The threat appears to be stable, but it could change suddenly.[2]

We can nevertheless draw cyber security lessons from the Russian invasion of Ukraine.[3] Although there has been no major disruption in the Netherlands, our allies have been hit by substantial war-related digital attacks,[4][5] many of them carried out by non-state actors such as hacktivists.

Public disquiet

The report that the Russian invasion of Ukraine could also affect Dutch digital security entered into Dutch households through various media.[39] At that time, the Dutch public regarded a possible cyber attack as the second greatest threat to security and general prosperity in Europe.[4]

The NCSC-NL, CSIRT-DSP and DTC also received many questions at that time on the effects of the war on Dutch digital security, both at a well-attended joint webinar[5] and through the usual communication channels.

Cyber security lessons

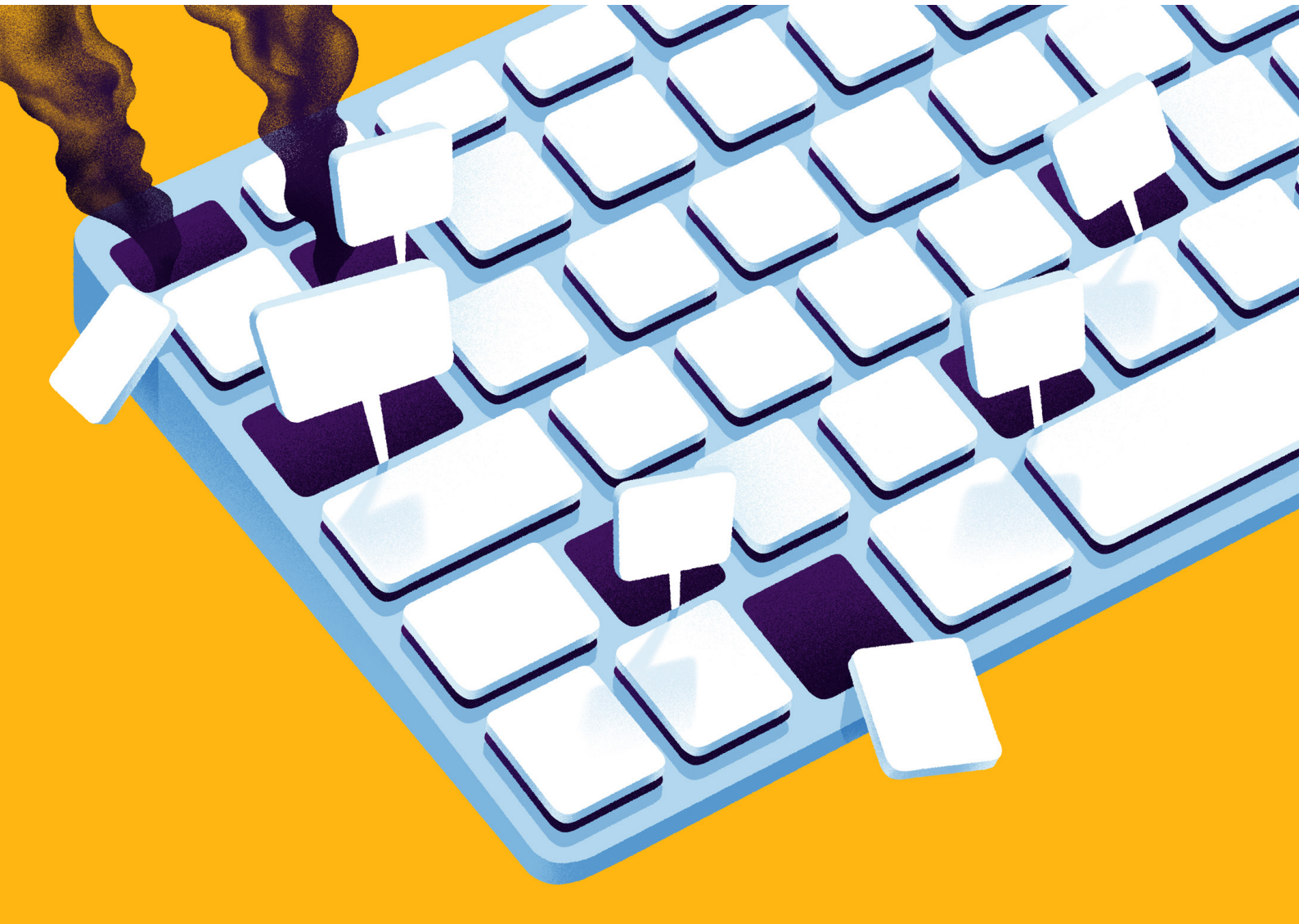
As so much has already happened in connection with the war, in the form of digital attacks and the measures taken to improve digital resilience, it is important in our view to take a retrospective look and draw lessons. That is what we do in this report.

The four main lessons are as follows:

1. **The rise of hacktivism:** hacktivists are a major presence in the context of the Russian invasion of Ukraine, carrying out disruptive digital attacks.
2. **The role of private-sector organisations:** private-sector organisations play an important role in improving the digital resilience of organization in and outside Ukraine. Private-sector organisations are, moreover, key in keeping vital services available.
3. **Getting the basics in order:** the rapid escalation of the war shows how important it is to be prepared for a future, rapidly escalating cyber crisis.
4. **Spillover effects:** cyber attacks are not confined within national borders; they can have an international impact.

This report discusses the four cyber security lessons and provides perspective for action with each lesson, enabling organisations to improve their digital resilience still further.

1. The rise of hacktivism



Lesson 1: hacktivists are a major presence in the context of the Russian invasion of Ukraine, carrying out disruptive digital attacks.

Hacktivists have carried out many digital attacks since the start of the Russian invasion of Ukraine.[6] Hacktivists are roughly divided into pro-Ukrainian and pro-Russian groups. Soon after the Russian invasion, for instance, the Ukrainian authorities called upon cyber specialists to join a new Ukrainian IT army that operates in allegiance with Ukrainian interests.[7]

- **Hacktivists have nevertheless sometimes targeted organisations that were not directly involved in the conflict.** They have not only carried out digital attacks on organisations directly involved in the war; pro-Russian hacktivists have also targeted organisations merely because they are based in countries that support Ukraine.[8] Hospitals in the Netherlands, for instance, have been the targets of hacktivists' digital attacks.[1]

  Pro-Ukrainian hacktivists have attacked organisations for not showing enough support with, from their perspective, the Ukrainian cause.[9] Organisations are often designated as targets in response to a political development[10] and are often targeted from an opportunistic perspective.

- **Hacktivists often carry out digital attacks in response of a political development.** Hacktivist digital attacks took place, for instance, after new arms supplies to Ukraine were announced,[11] Soviet monuments were taken down,[12] or political decisions were made that were regarded as anti-Russian.[13] Hacktivist attacks are characterised by ideological rather than financial motives.

- **Hacktivists try to attract attention to their digital attacks.** They use strong rhetoric in their public communications to make their actions more powerful, choosing digital attack targets that have a symbolic value, e.g. the 2022 Eurovision Song Contest.[14]

- **Many hacktivist groups are ad hoc organized.** The hacktivist group Killnet, for instance, uses Telegram channels to keep in contact with its supporters. Its Telegram channels have tens of thousands of users, who are not necessarily all hacktivists: cyber security researchers and journalists also closely monitor the group through these channels.

Potential impact on Dutch organisations

- **The impact of hacktivist attacks varies.** This is due to the ad hoc composition of hacktivist groups, which makes coordination and collaboration more difficult for hacktivists than e.g. for sophisticated state actors. It also changes the capabilities and level of expertise available.

- **An organisation's political position is a risk factor.** If an organisation has a political stance, that makes it a potential target for hacktivists, and this should be taken into consideration in your risk analysis.

- **Dutch digital infrastructure has been abused for DDoS attacks on Ukrainian websites.**[15] A good deal of internet traffic passes through the Netherlands because of the high quality of the Dutch digital infrastructure and the country's central location at many international internet hubs. Malicious actors can take advantage of our high-quality infrastructure to carry out digital attacks.

- **Hacktivism originating in the Netherlands can cause undesirable reactions.** Hacktivist attacks originating in the Netherlands can have adverse consequences, for example causing the country to be targeted by politically motivated counteractions. Abuse of the Dutch infrastructure is also bad for the country's international reputation.[16]

- **Hacktivist interference makes the threat landscape more complex.** State actors can conceal their own activities e.g. by ascribing them to hacktivist attacks.[17]

- **Carrying out digital attacks is a criminal offence.** This applies equally to hacking into computers or servers and carrying out a DDoS attack on a website. These rules apply to anyone in the Netherlands committing such offences.[18]

- **Being involved in hacktivism can also cause problems for people holding confidential government positions.** E.g. ties with hacktivist groups might become problematic when someone tries to obtain a security clearance.[19]

Perspective for action

Include DDoS attacks in your threat analysis.

Hacktivists use DDoS attacks in an attempt to disrupt the availability of digital systems and processes. DDoS attacks are a common attack technique used by hacktivists.

Include a DDoS scenario in your threat and risk analysis. The NCSC discusses how you can protect your organisation against a DDoS attack in its fact sheet "Continuïteit van online diensten" [Continuity of online services].

Check your crisis communication plan.

Hacktivists can also use a hack-and-leak operation to steal and leak confidential information to damage the reputation of an organisation or government body. They use defacement attacks to try to gain access to the target's communication channels and deface them with inflammatory, alarming and provocative texts.

Hacktivists' aim is to attract ample attention to their campaigns. Having carried out a digital attack, they actively publicise it, with the result that you may have to tackle questions from your stakeholders or e.g. the media.

A good crisis communication plan can help you to respond effectively to a digital attack, even if it attracts a lot of publicity.

The NCSC provides starting points for dealing with a digital incident in its publication "Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten" [Key points in crisis management and crisis communication in the event of digital incidents]

2. Private-sector organisations

Lesson 2: private-sector organisations play an important role in improving the digital resilience of organization in and outside Ukraine. Private-sector organisations are, moreover, key in keeping vital services available.

Private-sector organisations are playing an important role in securing the Ukrainian digital infrastructure and keeping it accessible. This has had a major impact on the organisations involved in the war, in various ways.

- **Private-sector organisations have been pivotal in keeping Ukrainian digital services accessible.** Ukrainian government bodies have frequently been affected by digital attacks. Thanks to private-sector organisations such as internet service providers, cyber security organisations, cloud service providers and hosting organisations, the Ukrainian population has been able to enjoy continued access to digital services. This has been possible partly because the Ukrainian authorities have moved data and servers outside Ukraine to keep them out of the hands of the Russian occupiers.[21]

- **Threat information from private-sector organisations has enabled digital attacks to be halted at an early stage.** On 15 January 2022, for instance, Microsoft reported destructive malware WhisperGate targeting various organisations in Ukraine, which it had discovered on 13 January 2022.[22] Based on this information, many organisations took appropriate action to prevent damage in Ukraine and elsewhere.[23]

  Other organisations such as ESET,[24] SentinelLabs,[25] Mandiant[26] and Palo Alto's Unit42[27] have helped to keep many organisations digitally secure by providing threat information.[28]

- **Internet service providers (ISPs) have been able to keep the internet accessible in Ukraine.** The Ukrainian internet infrastructure has been severely damaged by Russian physical[29] and digital[30] attacks. In addition, Russia diverts internet traffic into occupied areas via Russian servers for surveillance and censorship purposes.[31] This affects the availability, confidentiality and integrity of the internet for organisations and people in Ukraine.

  Russia often found it difficult to cause major disruption, because Ukraine has many different ISPs. A particular network going down had a relatively small impact on the system as a whole.[32]

  Satellite communication also played an important role in keeping the internet available in Ukraine. SpaceX activated its Starlink satellite network over Ukraine on 27 February 2022, at the request of the Ukrainian authorities.[33][34] This restored access to the internet in the areas severely affected by the war, and Ukrainian troops, civilians and organisations were able to stay in contact with the outside world.

- **Private-sector organisations make a valuable contribution by obeying sanctions and legislation.** This joint contribution ensures that the sanctions against Russia and Belarus are effective.[35]

Potential impact on Dutch organisations

- **Thanks to close collaboration with the private sector, many organisations have been able to improve their digital resilience.** This is true of government bodies both in Ukraine and elsewhere. Collaboration and knowledge sharing with the cyber security community is vital to keep digital systems secure.

- **Private-sector organisations can be targeted by digital attacks if they provide support to a warring party.** It is not only states that are involved in a conflict; technology companies also have substantial geopolitical sway as a result of the digital services and products that they provide. That influence can also make them potential targets of digital attacks.[36]

Perspective for action

Include hacktivists reactions in a risk analysis when your company makes a political statement.

Dutch public[37] and private-sector organisations are providing support to Ukraine in the fight against the Russian occupiers. That support may be desirable for all sorts of reasons. Include any negative side-effects as hacktivists reactions (such as DDoS-attacks) in a risk analysis.

Include the threat of digital attacks by hacktivists and state actors in your risk analysis. The threat can increase if your organisation provides support to Ukrainian organisations or speaks out against the invasion.

Work together with other organisations.

Together organisations have more knowledge than if they act on their own: for instance, they can enter into a partnership to exchange threat information or knowledge and experience. Active participation in various partnerships and consultative forums – also during periods when the threat level is lower – can provide a firm foundation for collaboration in times of crisis.

Active participation in partnerships such as an ISAC (sectoral consultative cyber security forum) or OKTT (organisation that provides objective threat information) contributes to the digital resilience of all participants. More information on launching and developing partnerships can be found on the websites of the NCSC and DTC.

3. Getting the basics in order

Lesson 3: the rapid escalation of the war shows how important it is to be prepared for a future, rapidly escalating cyber crisis.

The digital war has shown how important it is for an organisation to have its basic cyber security in order.

- **It was initially unclear what influence the Russian invasion of Ukraine was having on Dutch digital security.**[38] The potential effects of invasion-related digital attacks were also on the agenda of various media by the end of February,[39] and there was a good deal of uncertainty among the Dutch public at that time about a possible digital attack.[4]

  At that time the NCSC-NL, DTC and CSIRT-DSP did not have any evidence of digital attacks arising from the war in Ukraine that could have an impact on the Netherlands. At the same time, future digital attacks on Dutch organisations could not be ruled out either.[40]

- **Ukrainian organisations were able to limit the damage to a large extent thanks to good cyber defence.** The impact of the many digital attacks perpetrated on Ukraine was relatively limited.[41] Ukrainian organisations were found to be effective in **monitoring** digital attacks and **responding quickly**. They swiftly responded to malware and patched vulnerabilities, for instance, thus substantially limiting damage from digital attacks.[42]

  Many organisations in Ukraine also made **backups** in the cloud and moved services there right from the start of the war, so that data and digital processes were not solely reliant on local systems. In addition, the fragmented Ukrainian communications network protected various vital services thanks to **redundancy.**[43]

- **Digital attacks during the war often targeted vulnerable peripherals.** Attackers took great advantage of vulnerable peripherals to step up the rate of digital attacks. Abuse of vulnerable peripherals is more scalable than phishing attacks, which are time-consuming. Abused targets include vulnerable firewalls, routers and email servers.[44]

Potential impact on Dutch organisations

- **Many different war-related digital attacks have been carried out.** The NCSC kept track of them in a timeline in 2022.[45] The digital attacks differ in terms of attack methods and intended effects, which is a challenge when it comes to improving organisations' resilience.

- **Not all digital attacks are directly visible.** The fact that we do not observe digital attacks does not mean that they do not exist: for instance, attackers can take up positions in systems and only cause disruption later. Some basic measures (e.g. network segmentation and collecting log information) are effective even if an attacker already has access to a system.

Action strategies

Use scenarios in your risk analysis.

Digital attacks are difficult to predict. The attack methods used and the intended effects of digital attacks can differ. By using scenarios specific to your organisation, you can identify the different types of digital attacks that could affect you. Scenarios can help you to identify the impact of digital attacks and your organisation's resilience to them.

The NCTV and NCSC's Cyber Security Assessment Netherlands provides information on the digital threat, the interests that could be affected, our resilience and finally the risks, focusing on national security. This publication is useful when modelling threat scenarios or carrying out risk analyses.

The AIVD, MIVD and NCTV's Threat Assessment of State Actors provides valuable information on threats arising from state actors. This publication provides a useful basis for designing threat scenarios.

Take at least the basic cyber security measures.

Uncertainty about whether the digital threat will manifest itself, and if so, how, shows the need to have your digital security in order. Both the NCSC and DTC have produced two guides that are useful, depending on the organisation's level of maturity, in improving digital resilience.

In its guide "Five basic principles of secure digital entrepreneurship" the DTC discusses security principles that help businesses to improve their digital resilience.

In its "Guide to cyber security measures" , the NCSC discusses the eight basic measures needed to protect your organisation against digital threats.

4. Spillover effects

Lesson 4: cyber attacks are not confined within national borders; they can have an international impact.

The digital attacks carried out in the context of the Russian invasion of Ukraine have mainly hit organisations in Ukraine, bordering countries that used to be part of the Soviet Union, and Russia itself. Some of these digital attacks have had broader spillover effects.

- **Disruption of one digital product or service can cause major disruption to one or more products or services, or even their complete failure.**[46] If a Dutch organisation relies on a digital product or service and that drops out due to a digital attack on a supplier elsewhere, we refer to this as a 'spillover effect'.

- **Many organisations have a limited understanding of what digital products and services they rely upon.** This was revealed e.g. by the Log4J crisis in December 2021.[47] Because of these complex digital services, it is difficult to foresee how knock-on effects could manifest themselves.

- **Spillover effects can be intentional or unintentional.** An attacker may deliberately target a digital product or service in order to cause large-scale disruption; alternatively, a knock-on effect may be unintentional, when a digital attack causes unforeseen side effects.

- **These spillover effects were most clearly apparent in the digital attack on Viasat.** Viasat is a satellite communication services provider.[48] Tens of thousands of Viasat modems were hit by a digital attack on 24 February 2022, the day when the Russian invasion of Ukraine started. As Viasat provides services to both military and civilian users,[49] the disruption due to the digital attack was noticeable far beyond Ukraine: thousands of wind turbines in Europe temporarily went offline,[50] for example, and the internet was inaccessible for a while in some remote areas.[51]

- **Disinformation was also disseminated in Ukraine as a result of a digital attack on a supplier.** Seventy Ukrainian government websites were defaced with alarming texts in the night of 13–14 January 2022, for instance, because a joint supplier had been hit by a digital attack.[52]

The impact on Dutch organisations

Being a small, open trading country, the Netherlands is highly interdependent on foreign countries, and it relies on international trading and production chains.[53] This is also the case with digital products and services, as many Dutch organisations are reliant on foreign suppliers.

- **The Netherlands' international orientation and integration is not without risk.** It can be difficult to maintain an overview of all our suppliers of digital services and products. If an international supplier is compromised, that can have effects in the Netherlands. In addition, malware – if systems are not properly segmented – can spread to Dutch systems from a system in another country.

- **Spillover effects are often impossible to predict or foresee.** Failure of a digital product or service can cause a chain reaction that is difficult to predict, because of the complexity of many information systems.

Perspective for action

Segment your networks.

By segmenting your network, you limit the consequences of a digital attack. Segmenting means dividing a network into multiple zones, making it more difficult for an attack on part of your organisation or one of your suppliers abroad to spread to your network.

The basic measures set out by the NCSC explain the importance of network segmentation. The Dutch ISP KPN outlines how to carry out network segmentation in a blog. The American National Institute of Standards and Technology sets out the structure of a segmented network in detail in "SP 800-215".

Apply Zero Trust principles in your IT infrastructure.

Applying Zero Trust principles creates various layers of defence in your network segments. The Zero Trust model is based on the assumption that network traffic is basically untrustworthy and must therefore always be verified. That makes it more difficult for attackers to move laterally across a network.

For more information about Zero Trust and how to apply these principles to your systems see the NCSC fact sheet "Prepare for Zero Trust" and the expert blog "What about zero trust?".

Examine your supply chain.

A software supply chain comprises all the codes, people, systems and processes involved in developing and implementing your software. Undesirable dependencies in it can make your organisation particularly vulnerable to threats arising from a political conflict: for example, suppliers in other countries may be rendered unavailable as a result of a boycott or digital attack. Suppliers can also be susceptible to undesirable political interference, so include that in your risk analysis.

An understanding of the systems and software being used in your organisation, and restricting access to them to the absolute minimum necessary, will protect against cyber incidents spreading within a supply chain. Incidents in your supply chain can cause problems for your organisation even if the incident does not spread to you. The Digital Trust Center provides a guide to agreeing measures with IT suppliers.

Install software updates promptly.

Digital attacks can be carried out on a large scale if there are unpatched vulnerabilities. Prompt patching ensures that attackers have limited time to abuse vulnerabilities, thus reducing the likelihood of a prior digital attack spreading to your systems.

Installing software updates is one of the "basic cyber security measures". For more information see the websites of the NCSC and DTC.

References

The University of Amsterdam and the Netherlands Defence Academy produced a publication at the end of 2022 that looks in detail at digital warfare during the war in Ukraine.

> See the paper "The 'Next' War Should Have Been Fought in Cyberspace, Right?" ?" by Paul Ducheine, Peter Pijpers and Kraesten Arnold.[3]

In addition, the NCSC is producing a new series of the "Enter" podcast, in which it, along with NCSC staff, cyber experts and other stakeholders, discusses how the Netherlands has dealt with the war in Ukraine and the associated cyber security issues.

> The NCSC's "Enter" podcast can be accessed via Spotify and Apple podcasts.

[1] "DDoS-aanvallen treffen aantal ziekenhuizen", [Several hospitals hit by DDoS attacks], Z-CERT, viewed 31 January 2023.

[2] "Digitale aanvallen oorlog Oekraïne", [Ukraine war digital attacks], NCSC, 31 March 2022.

[3] Ducheine, Pijpers and Arnold, "The 'Next' War Should Have Been Fought in Cyberspace, Right?"?", Amsterdam Law School Legal Studies Research Paper No. 2022-47, 2022.

[4] This is clear from research carried out by Clingendael (the Netherlands Institute of International Relations) following the Russian invasion of Ukraine.

Monika Sie Dhian Ho, Mark Elchardus, Christopher Houtkamp and Teun van der Laan, "Tussen hoop en vrees" [Between hope and fear], Clingendael, 30 December 2022.

[5] "Webinar: Huidig beeld en digitale impact oorlog Oekraïne" [Webinar: Current situation and digital impact of Ukraine war], NCSC and DTC, 9 March 2022.

[6] The word 'hacktivism' is a fusion of 'hacking' and 'activism'. Hacktivists are non-state actors who carry out digital attacks with activist aims based on ideological motives.

[7] James Pearson, "Ukraine launches 'IT army,' takes aim at Russian cyberspace", Reuters, 27 February 2022.

[8] "Pro-Russian Hacktivist Groups Target Ukraine Supporters", Intel471, 14 September 2022.

[9] Pierluigi Paganini, "Anonymous targets western companies still active in Russia", SecurityAffairs.co, 24 March 2022.

[10] Sergiu Gatlan, "Pro-Russian hacktivists take down EU Parliament site in DDoS attack", BleepingComputer, 23 November 2022.

[11] An airport website in the USA was the target of a n DDoS-attack. Responsibility for it was subsequently claimed by Killnet, a pro-Russian hacktivist actor, which carried out the attack in response to American arms supplies to Ukraine.

[12] Estonia repelled a major DDoS attack after the country took down a number of Soviet monuments. These attacks are thought to have been carried out by the hacktivist group Killnet.

Andrius Sytas, "Estonia says it repelled major cyber attack after removing Soviet monuments", Reuters, 18 July 2022.

[13] In various countries, including Italy, Lithuania, Finland and Latvia, digital attacks were carried out in response to a development regarded as anti-Russian.

[14] Mike Moore, "Eurovision 2022 was targeted by Russian hackers", TechRadar, 16 May 2022.

[15] 360Netlab, Twitter, 16 February 2022. https://twitter.com/360Netlab/status/1493797519725367302

[16] "De oorlog in Oekraïne en onze nationale veiligheid" [The war in Ukraine and our national security], NCTV, 30 March 2022.

[17] Parliamentary paper 3891936, "Stand van zaken cyber security in relatie tot het conflict in Oekraïne" [The cyber security situation in relation to the conflict in Ukraine], 11 March 2022.

[18] "Oorlog Oekraïne" [Ukraine war], Het Openbaar Ministerie (Public Prosecution Service), viewed 30 January 2023.

[19] "Wanneer vindt er een veiligheidsonderzoek plaats?" [When does security vetting take place?], Rijksoverheid (Dutch Government).

[20] "#Cloud4Ukraine", Dutch Cloud Community, viewed 31 January 2023.

[21] Eric Geller,"Ukraine prepares to remove data from Russia's reach", Politico, 22 February 2022.

[22] The malware was WhisperGate, destructive software designed to damage the Master Boot Records (MBRs) of the systems affected, rendering them permanently inoperable.

"Destructive malware targeting Ukrainian organizations", Microsoft, 15 January 2022.

[23] Joyce Hakmeh and Esther Naylor, "How the tech community has rallied to Ukraine's cyber-defence", The Guardian, 7 March 2022.

[24] "UA Crisis", ESET

[25] "Ukraine response", SentinalOne.

[26] "Ukraine crisis resource center", Mandiant.

[27] Unit42. https://unit42.paloaltonetworks.com/

[28] The list is not exhaustive: many other organisations and research institutes not mentioned here have shared valuable threat information and thus helped to produce a joint threat assessment.

[29] Thomas Brewster, "Ukraine's engineers battle to keep the internet running while Russian bombs fall around them", Forbes, 22 March 2022.

[30] Chris Vallance, "Ukraine war: Major internet provider suffers cyber-attack", BBC, 28 March 2022.

[31] Matt Burgess, "Russia is taking over Ukraine's internet", WIRED, 15 June 2022.

[32] Emile Aben, "The resilience of the internet in Ukraine", RIPE Labs, 10 March 2022.

[33] Ukrainian vice prime minister Mykhailo Fedorov asked SpaceX CEO Elon Musk to activate Starlink over Ukraine and Ukrainian terminals on 26 February 2022.

Callie Patteson, "Ukrainian vice prime ministers asks Elon Musk for Starlink satellites as Russia invades", New York Post, 26 February 2022.

[34] Sam Raskin, "Elon Musk activates Starlink in Ukraine after vice prime minister's plea", New York Post, 27 February 2022.

[35] "Nederlandse uitvoering sancties tegen Rusland en Belarus" [Dutch implementation of sanctions against Russia and Belarus], Rijksoverheid.

[36] Maciej Góra, Ewelina Kasprzyk, Eliza Kotowska and Michał Krawczyk, "The twilight of the neutrality of digital technology", The Kosciuszko Institute, 2023.

[37] "Nederlandse hulp voor Oekraïne" [Dutch help for Ukraine], Rijksoverheid.

[38] Cf. the concept of 'the fog of war', which refers to situational uncertainty about military operations: "War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth." Carl von Clausewitz, "On War", 1832, (ed. Peter Paret, 1989), 101.

[39] The chat show Op1, for example, devoted ample attention on 25 February 2022 to the uncertain effects of a possible 'cyber war'.

"Ronald Prins over de onzichtbare cyberoorlog" [Ronald Prins on the invisible cyber war], Op1, 25 February 2022.

[40] "Digitale aanvallen oorlog Oekraïne" [Ukraine war digital attacks], NCSC, 26 February 2022.

[41] John Bateman, "Russia's wartime cyber operations in Ukraine: Military impacts, influences and implications". Carnegie Endowment, 16 December 2022,

[42] James Lewis, "Cyber War and Ukraine", Center for Strategic and International Studies, 16 June 2022.

[43] Nick Huber, "What Ukraine's cyber defence tactics can teach other nations", Financial Times, 9 November 2022.

[44] Andy Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless", WIRED, 10 November 2022.

[45] "Digitale aanvallen Oekraïne: een tijdlijn" [Digital attacks on Ukraine: a timeline], NCSC.

[46] Knock-on effects: Eric Luiiff en Marieke Klaver, "Afhankelijkheden en keteneffecten"[Dependencies and knock-on effects], Magazine Nationale Veiligheid en Crisisbeheersing, 2015.

[47] "Log4J", NCSC.

[48] Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", WIRED, 23 March 2022.

[49] Ellen Nakashima, "Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say", The Washington Post, 24 March 2022.

[50] Maria Sheahan, Christoph Steitz and Andreas Rinke, "Satellite outage knocks out thousands of Enercon's wind turbines", Reuters, 28 February 2022.

[51] "KA-SAT Network cyber attack overview", Viasat, 30 March 2022.

[52] "Фрагмент дослідження кібератак 14.01.2022", CERT-UA, 26 January 2022.

[53] "Nederland handelsland 2021" [Dutch Trade in Facts and Figures, 2021], CBS, 14 September 2021.

Published by
National Cyber Security Centre
(NCSC)
PO Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

March 2023