Report-out Learning Journey Poland

How public-private partnerships can contribute to a safe and resilient Netherlands

22 – 25 June 2026

National Coalition for Security and Resilience
'The Vanguard'

PARTICIPATING ORGANIZATIONS POLAND 2026:

TABLE OF CONTENTS

Our journey to Poland

Dear participants,

The study trip to Poland left a lasting impression. Upon our return, we found the Netherlands in the grip of a brief ‘Code Red’ heatwave, but in Poland we saw what it means to have to demonstrate increased resilience over a longer period. In Poland, they are attempting to achieve a level of resilience in a few years that took Finland decades to attain. Some of us therefore returned with ‘a knot in our stomachs from the sense of urgency felt by the Poles’. In Poland, war is seen as almost inevitable. With this sense of urgency in mind, we therefore agreed on a number of concrete action points together on the final day. There is a widespread sense of responsibility within the group to commit ourselves, both personally and on behalf of the organizations we represent, to enhancing the Netherlands’ resilience. During the systemic collaboration session on Wednesday, we also worked together to better define the approach we are taking as participants in this group. This will help us to develop even more concrete actions.

We realized in Warsaw that we are a unique group of organizations. The Poles were surprised by the natural and flexible way in which public and private organizations consult and collaborate with one another. Such accessible cooperation between so many different types of actors is virtually unthinkable in Poland. There, a much stronger top-down approach prevails. This provides a great deal more clarity but does not always fit with our ‘polder’ approach. So the trick is to combine the Vanguard’s bottom-up approach with greater clarity about what is decided top-down in a crisis or war. This is another area that we, as the Vanguard, will be focusing strongly on in the coming period.

Being self-reliant together is not only a noble aim but also requires practical training. Many participants were therefore impressed by the ‘be ready’ training and wish to explore how we can expand resilience training in the Netherlands. The issue of disinformation has also been embraced by our group. Combating this requires action from both the public and private sectors. This helps to ensure that our society becomes and remains self-reliant together.

The aim of working together to achieve collective resilience also applies to relations between countries. This sentiment came across very clearly during the well-attended peer-to-peer dinner on Tuesday evening. The Vanguard expressed its gratitude for how Polish soldiers had saved and liberated Dutch territory during the Second World War. In response, the Polish organizations spoke emotionally about the Dutch efforts in shooting down Russian drones over Polish territory. They were also struck by the fact that it was Dutch organizations, in particular, who had come to seek them out to learn from them. All of this gives them the feeling that they are not on their own. And that was precisely the message with which our delegation concluded the evening: you are not alone. This applies to Poland and the Netherlands as NATO allies and economic partners. But it also applies to all members of the Vanguard group. None of us can do it alone. And none of us has to do it alone.

Let us continue to work together in the coming period to become more resilient.

Summary key insights, reflections, and next steps

Insights

- Poland is a **frontline** state where **hybrid warfare** is already underway: cyber, sabotage, disinformation and drones are intertwined. The threat is concrete, from years of espionage to the first destructive attack on the energy sector at the end of December 2025.
- The **sense of urgency** is deeply and broadly rooted, visible in daily life and education. This is immediately the biggest difference with the Netherlands, where the urgency is still too low.
- The approach is **central and top-down**: one front door for citizens and businesses, centrally supplied tools and the RCB as the coordinating pivot. In contrast to the Dutch bottom-up culture, the conclusion is: we need both.
- **Civil and military** are strongly intertwined and firmly anchored. Resilience is not a non-committal choice, but organized and mandatory.
- **Citizen resilience** is highly developed, physically and mentally. As the Poles said: putting together an emergency kit is not difficult, talking about it with your loved ones is.
- **Disinformation** is an integral part of hybrid warfare, with its own analysis center and rapidly growing AI influence. The Netherlands is visibly lagging behind here.
- **Investing in people** is a strong point: Poland recruits up to primary education and builds prestige. A concrete learning point for the Netherlands.

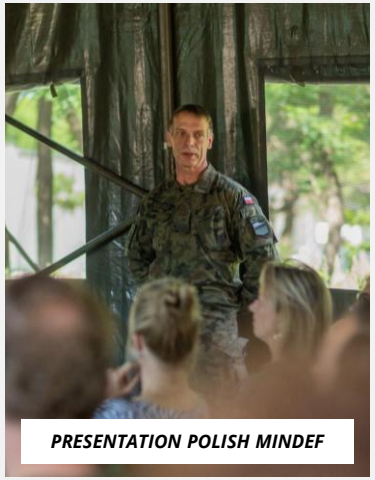
Next steps

- We will come back with a **concrete action** list and **clear triggers**. The focus is not only on new initiatives, but especially on accelerating and scaling what is already running.
- **5 actions** have been identified for the coming period:
    1) **Disinformation**: Digital resilience is strengthened by bringing fragmented initiatives together centrally in a public-private partnership. A small coalition will start under the leadership of TNO to scale up the approach broadly in September.
    2) **Citizen resilience and Be Ready-training**: The resilience of citizens and companies will be boosted through an accessible training offer based on the Polish model. Participating organizations are developing an integrated package for this and deploying internal reservists as trainers.
    3) **Reservists and critical infrastructure**: Vital organizations set up their own pool of "vital infrastructure reservists" to safeguard critical functions and relieve the burden on the Ministry of Defense. This plan and the link to Article 5 scenarios will first be coordinated with the Ministries of Infrastructure and Water Management and J&V.
    4) **Agenda, urgency & positive narrative**: The sense of urgency is increased by strategically placing resilience on the agenda of Boards of Directors. This initiative is supported by active sponsorship from CEOs and a positive narrative around sovereignty.
    5) **Accelerating Resilient Stores**: A total of 1,000 supermarkets are being physically and operationally prepared for large-scale power outages. Together with municipalities and security regions, the emergency power facilities and logistical safety are being set up for this purpose.

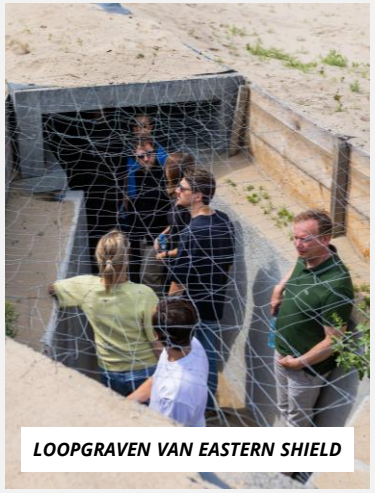
1. Looking back on the learning journey

LOOKING BACK ON THE LEARNING JOURNEY

In four days we got to know Poland, its security ecosystem and each other better.



PRESENTATION POLISH MINDEF



LOOPGRAVEN VAN EASTERN SHIELD

'BE READY' TRAINING BY THE TDF

DINNER AT THE AMBASSADOR'S RESIDENCE

SYSTEMISCH SAMENWERKEN MET SIETS BAKKER

DINNER WITH 25 POLISH ORGANISATIONS

PRESENTATION RCB

EMBASSY OF THE NETHERLANDS IN WARSCHAU

PRESENTATION POLISH CYBER COMMAND

SPEECH ROBERT KLONOWSKI

FROM INSIGHT TO ACTION

LOOKING BACK ON THE LEARNING JOURNEY

27 organizations went on an exploratory mission to Poland together with clear objectives and questions

MAIN QUESTION

What can we learn from the Polish ecosystem of resilience and security and how can we translate this into actions in the Netherlands?

GOAL 1: THE BASIS

Strengthening mutual trust

GOAL 2: LEARN

Gaining insight into the Polish ecosystem and PPP

GOAL 3: REFLECT

Reflect on the ecosystem in the NL and PPP

GOAL 4: ACT

Actions in the Netherlands

LOOKING BACK ON THE LEARNING JOURNEY

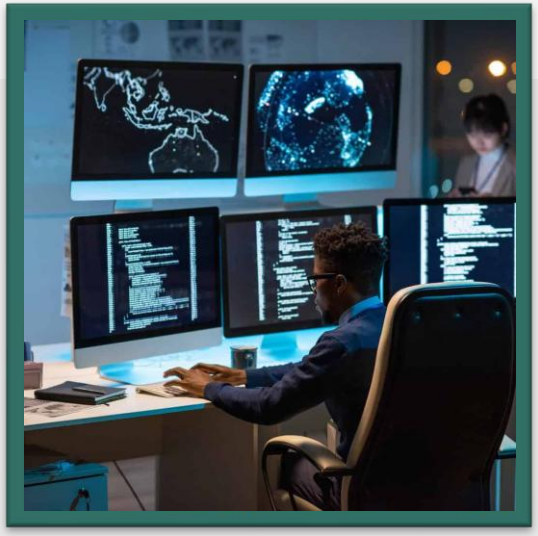
During the journey we explored a different theme every day

MONDAY

FOOTHOLD IN WARSAW

Start the week with a Dutch reception in Poland

TUESDAY



A DAY FULL OF POLISH INSIGHTS

Gain insight into Poland's security and resilience system, focus on cybersecurity and disinformation

WEDNESDAY

BEYOND THE THEORY

Learn about military preparedness in Poland and gain deeper insights of cooperation within the Vanguard

THURSDAY

FROM POLISH INISGHTS TO DUTCH ACTIONS

Identify and work on the joint next steps that we will take in the Netherlands

LOOKING BACK ON THE LEARNING JOURNEY

Weekly program

MONDAY

RECEPTION AT THE EMBASSY & INTRODUCTIONS

- Reception & presentation at the Embassy of the Kingdom of the Netherlands
- Dinner at the ambassador's residence

TUESDAY

POLISH SECURITY & RESILIENCE

- RCB (Government Centre for Security)
- Poland Cyber Command
- Ministry of Digital Affairs + NASK
- Walking tour through the old town
- Peer-to-peer dinner

WEDNESDAY

MILITARY READINESS & COLLABORATION

- Ministry of Defense & Territorial Defense Forces
- Eastern Shield tour
- ‘Be Ready’ training
- Systemic collaboration
- Reflection walk
- Vanguard dinner

THURSDAY

FOLLOW-UP FOR A RESILIENT NETHERLANDS

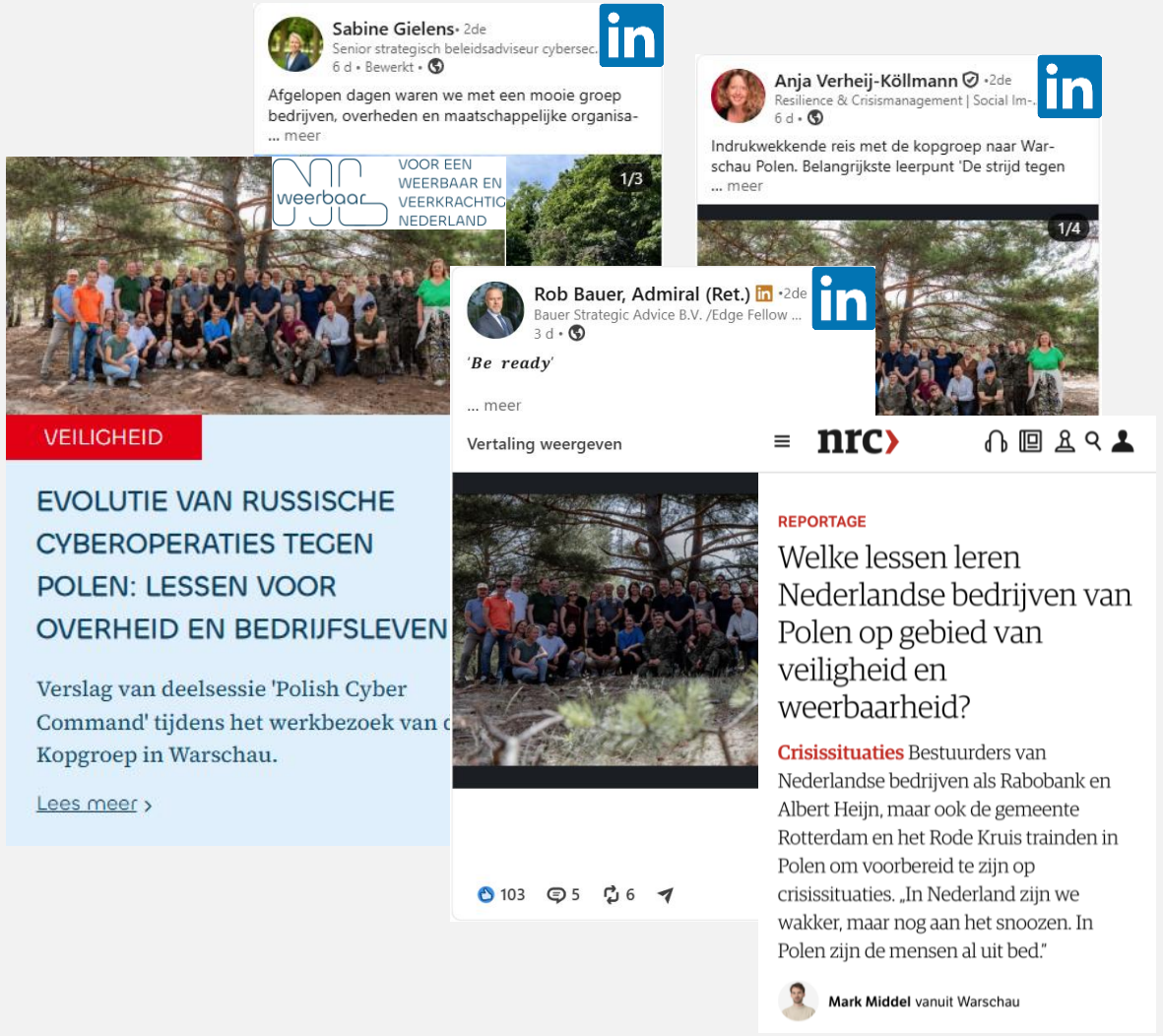
- From insight to action
- Joint closure
- Roundtable interview Dutch national newspaper

Insights and reflections from the study trip have been published in various ways

To raise awareness of the urgency of the situation in the Netherlands, it is essential to reach out actively, engage in dialogue and share the lessons we have learnt widely. By communicating our journey and our mission through various channels, we are building the necessary public support and offering a concrete way forward.

The insights from the study trip were shared through the following channels:

- **WeerbaarNL:**
  - Throughout the learning journey, Anja Verheij posted several articles about the Vanguard and the learning journey on WeerbaarNL
    - See Appendix for the links
- **Media coverage:**
  - Thursday afternoon there was a round table interview with the NRC correspondent in Poland about the Vanguard and our learning journey
  - Link to the article
- **LinkedIn:**
  - Several posts on LinkedIn have also gained a lot of traction



2. Key insights

KEY INSIGHTS

Reception and dinner at the Embassy of the Kingdom of the Netherlands

Insights

- The program opened on Monday evening at the Dutch Embassy in Warsaw, with a welcome and a short keynote address by Ambassador Jennes de Mol on the historical and current context of Poland and its cooperation with the Netherlands.
- De Mol has been ambassador to Poland and Belarus since 2024, and prior to that served as ambassador to Ukraine for five years, right through the 2022 invasion. Having previously held posts in Moscow and St Petersburg, he is able to interpret the geopolitical tensions and the Polish perspective on Russia from the inside.
- He immediately conveyed a sense of urgency and explained that resilience is deeply ingrained in society: friends train in survival skills and marksmanship at the weekend, and children are taught resilience and safety from primary school onwards.
- He also outlined the domestic challenges: strong polarization and a growing far-right movement are putting pressure on social cohesion and hampering effective policy-making and security.
- The most striking account concerned the Russian drones over Polish territory in September 2025, which were shot down in part by Dutch F-35s. It was the first time that NATO allies had shot down a threat over Polish airspace to defend it. In Poland this made a deep impression: the feeling of not being left to face a threatening situation alone. In the weeks that followed, thank-you notes poured in from all over Poland.

Impressions

KEY INSIGHTS

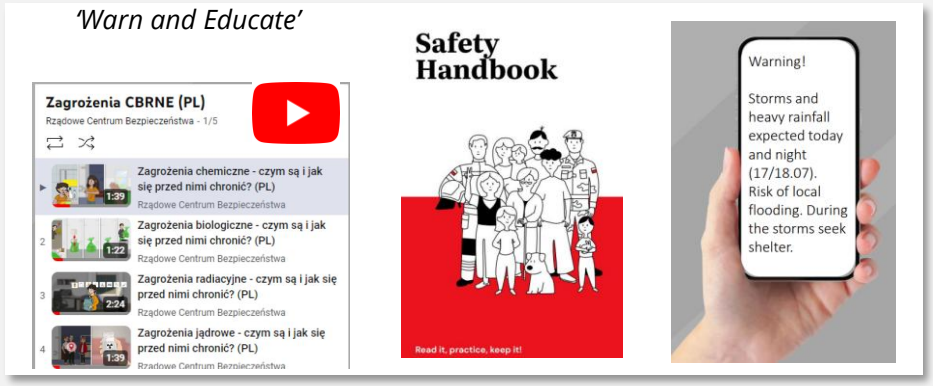
Presentation Government Centre for Security (RCB)

Insights

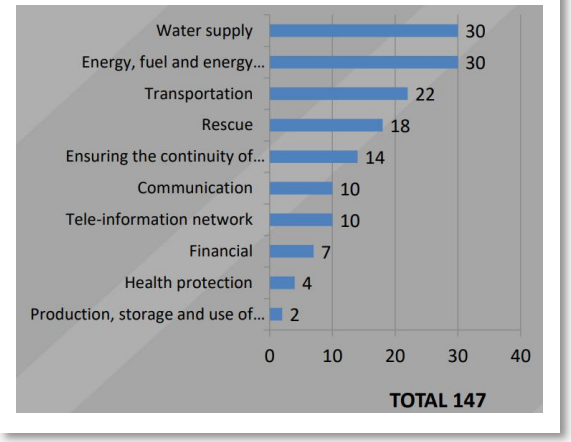
- The Rządowe Centrum Bezpieczeństwa (RCB), established in 2008, is the national crisis center reporting to the Prime Minister. It does not carry out crisis management itself, but rather coordinates, supports and provides information. Providing information is a key role: the RCB acts as the linchpin linking ministers, government departments, implementing bodies and critical sectors. As the national coordinator for resilience, the RCB adopts a whole-of-society approach that brings together citizens, public and private sector organizations, and the government. In addition, it maintains cooperation with the EU and NATO and develops evacuation plans for all voivodeships.
- The center monitors the situation 24/7 and provides situational updates, with particular focus on Ukraine and the eastern border with Belarus. Every year, hundreds of alerts are sent to citizens via Alert RCB in multiple languages, covering not only current events but also how to respond. Public preparedness is well developed (Safety Handbook, evacuation rucksack, RCB Safety Academy) and reaches the entire population through numerous channels (YouTube, social media, leaflets), including an educational campaign for children and teachers.
- The RCB actively verifies the authenticity of its own warnings on social media and the government website. In this way, resilience to disinformation is an integral part of crisis communication.
- For critical infrastructure (147 operators), responsibility for ensuring continuity of operations lies primarily with the operator itself. The RCB facilitates public-private partnerships, coordinates responses when critical infrastructure is under threat, shares threat intelligence and provides support. The RCB is in direct contact with the vital/critical sectors on these matters.
- The Polish approach demonstrates that effective communication must be transparent about real threats and always linked to a concrete plan of action to prevent public unrest. Sharing information works best when citizens are given a clear plan of action.

Impressions

'Warn and Educate'



Overview of the147 CI operators



KEY INSIGHTS

Presentation Polish Cyber Command

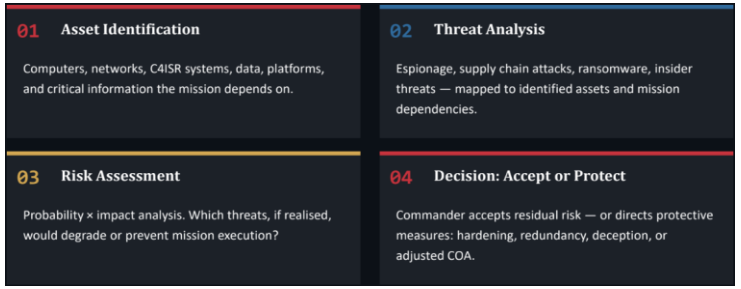
Insights

- Polish Cyber Command is the military cyber command responsible solely for cyber defense, not for offensive or intelligence operations, although it works closely with intelligence units. Russia is the main adversary, alongside Belarus, whilst the Netherlands focuses more strongly on China.
- The threat picture has escalated from espionage through disruption to destruction, with Russian operations having increased fivefold since 2022. On 29 December 2025, the first destructive attack took place: a wiper attack on more than 30 wind and solar farms and a large combined heat and power plant (serving approximately 500,000 customers), in the middle of winter. This mirrors the pattern of Russian attacks on Ukraine. Key takeaway: Look to Ukraine and take these escalations seriously.
- Civilian infrastructure (ports, airports, railways, logistics, IT) is a critical military dependency and therefore a target. The adversary shifted its focus from government and defense to civilian organizations holding the same data but with weaker defenses.
- Risk vectors lie primarily with civilian partners: compromised suppliers, GPS jamming and spoofing in northern Poland and at ports, and vulnerable IP cameras. The GRU tracked aid convoys to Ukraine via more than 10,000 cameras along supply routes.
- Cyber Mission Assurance (CMA) is their core process: making missions resilient by identifying assets and threats, assessing risk, and choosing between accepting or protecting them. The answer lies in civil-military cooperation with direct lines of communication and shared threat intelligence, voluntary as long as there is no war, and deliberately on-premises. The sharing of threat intelligence with civilians could still be improved in the Netherlands.
- Talent is a key strength: PCC has grown to over 6,000 staff through recruitment extending as far back as primary school, a prestigious image and favorable terms backed by government support. In addition, scarce cyber experts receive extra pay to ensure they remain with PCC. This presents a concrete lesson for the Netherlands.

Impressions

Parallel timelines of cyber threat in Ukraine and Poland

The 4 steps of Cyber Mission Assurance (CMA)



KEY INSIGHTS

Presentation Ministry of Digital Affairs

Insights

- Poland is building a **multi-layered cybersecurity framework** that combines regulations, coordination, personnel, funding and shared tools. The practical aim is to detect threats earlier, coordinate more quickly and keep public services running.
- The framework comprises four layers: **strategic** (political guidance via the Cybersecurity Council and a government representative appointed by the Prime Minister), **operational** (the PCOC framework in which CSIRTs, government departments, the police, the military cyber command and ministries respond rapidly), **system tools** (S46, cyber.gov.pl and shared services) and a **sectoral layer** of CSIRTs closely linked to the economic sectors.
- The ecosystem is **centrally organized** and the ministry provides cyber solutions to users. This prevents duplication of effort and gives smaller organizations access to more powerful tools. Here, too, Poland's centralized, top-down nature is evident.
- **cyber.gov.pl** serves as the **central platform** in this framework: a single government platform for citizens, businesses and institutions, offering incident reporting, alerts, knowledge and training all in one place, along with secure access via the National Node.
- Under the new legislation, **sectoral CSIRTs** will be established to support incident response within each economic sector and to connect stakeholders with the national CSIRTs. This is particularly relevant given the public-private nature of our Vanguard.
- Just as with the Polish Cyber Command (see slide 15), MINDIG is also strongly committed to people, through training and a fund for cyber talent.

Impressions

KEY INSIGHTS

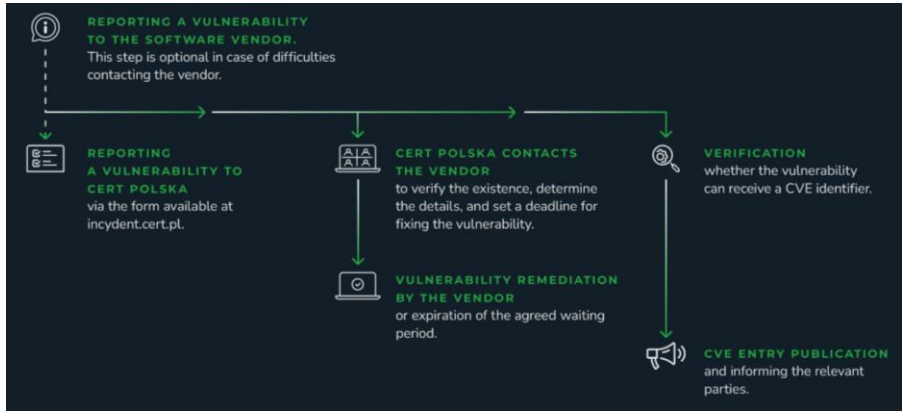
Presentation NASK (1/2): Organization and cyber threats

Insights

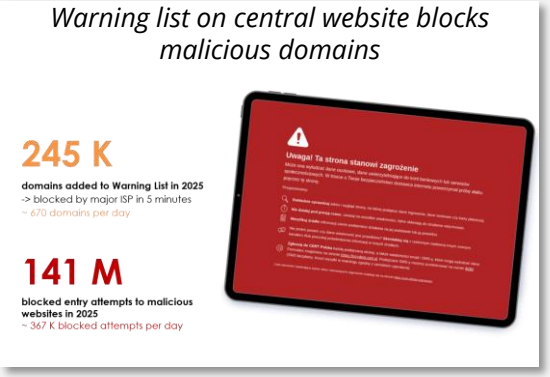
- NASK is the national research institute under the Ministry of Digital Affairs. It manages the .pl domain registry and hosts CERT Polska, which has existed since 1996 and has been carrying out the duties of CSIRT NASK since the 2018 Cyber Security Act.
- Poland has three national CSIRTs, each with its own legally defined remit and reporting obligations: CSIRT MON (defense), CSIRT GOV (government, central bank, critical infrastructure) and CSIRT NASK (the wider public: businesses, digital service providers, local authorities and citizens).
- The number of incidents rose sharply in 2025 (+152 per cent, over 206K). This is partly due to much improved detection, so it is not an entirely negative story. Every day, CERT Polska handles around 1,800 reports and 700 incidents.
- Phishing is by far the biggest threat (around 90%), alongside fake investment schemes. Smishing (phishing via text message and WhatsApp) and ransomware (+22%) are on the rise, with public awareness campaigns being rolled out as a countermeasure. The warning list of blocked domains is managed via the central moje.cert.pl portal. In the Netherlands, a great deal is already happening in this area in the private sector; for example, KPN is currently developing an anti-phishing shield.
- In late December 2025, the energy sector was hit by a major cyber incident, right in the middle of winter. The damage was limited, but it highlighted just how vulnerable critical infrastructure is at the worst possible moment.

Impressions

Vulnerability disclosure process within CERT Polska (NASK)



Warning list on central website blocks malicious domains



KEY INSIGHTS

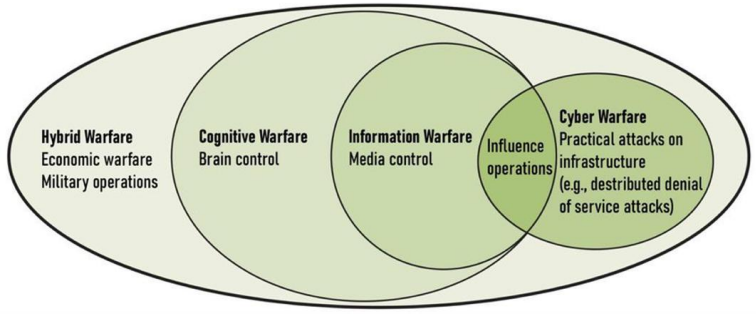
Presentation NASK (2/2): Disinformation Analysis Centre

Insights

- Within NASK, the Disinformation Analysis Centre analyses the information domain. Poland is described as a frontline state: the hybrid war with Russia and Belarus is already underway there, involving sabotage, drone incursions, cyber-attacks and large-scale influence operations, though it remains below the threshold of open warfare. Cyber threats and disinformation are currently being taken more seriously in Poland; we in the Netherlands will need to respond more proactively to this. Another distinctive feature of this Polish approach is its high degree of centralization, with a single clear point of contact, in contrast to the Netherlands, where there are various reporting centers.
- The center operates with four teams: continuous monitoring and rapid detection; analysis of narrative trends and fact-checking; external threat analysis (Russia and China); and analysis of campaigns and automation.
- Disinformation takes three forms: impersonation of public figures or institutions, manipulative content (often using AI) and outright false content. Recurring themes include anti-state sentiment, migration, social issues and health.
- The opponent's objective in Poland: to undermine support for Ukraine, erode trust in the US, NATO and the EU, and portray Poland as chaotic, under threat and internally divided.
- AI-driven influence operations are growing rapidly, as seen in the 'Operation Overload' campaign targeting Poland and NATO countries: imitation media brands, low-cost AI-generated content and bot networks designed to make a particular viewpoint appear widespread.
- Disinformation is traceable: from incident to online activity to dominant narratives to Russia's strategic objectives. Sometimes via controllable Russian actors, sometimes via 'useful idiots' who unwittingly serve the Russian agenda. Example: following the appearance of Russian drones over Poland, narratives quickly emerged claiming that Ukraine was dragging Poland into the war.

Impressions

Hybrid war in the cyber domain



KEY INSIGHTS

Peer-to-peer dinner

Insights

- The peer-to-peer dinner was attended by 27 Polish guests from 14 Polish organizations, including Polish Railways, various ministries, the Polish Red Cross and the City of Warsaw.
- The speeches, delivered by Sjoerd van der Smissen and Rob Bauer, amongst others, focused on the ties and shared history between the Netherlands and Poland.
- Sjoerd van der Smissen spoke of his respect and gratitude e for General Maczek, who liberated Breda from the Germans in 1944 and received a Dutch pension for the rest of his life. A gesture which the Poles still deeply appreciate to this day. Rob Bauer said that Poland would never stand alone again. This struck a chord and gave the evening a special significance.
- The Polish delegates also took the floor. They were surprised by our Vanguard and our model of public-private partnership, something that is unthinkable in the Polish context. They were visibly impressed and indicated that they could learn a great deal from it.
- Robert Klonowski (Deputy Director at the Department for Civil Protection and Crisis Management within the Polish Ministry of the Interior) was moved to tears during his speech: throughout his childhood, he had longed to leave oppressed Poland and set off for the free West. The fact that we, as a Vanguard, had now chosen to come to Poland touched him deeply. His speech was a turning point of the evening and indeed of the whole week.
- The dinner provided a unique opportunity for the direct exchange of knowledge. For instance, there was a very open exchange with a colleague from the Polish Red Cross, who shared their knowledge and experiences with us. This generous approach to sharing knowledge was characteristic of the atmosphere of the evening.

Impressions

Polish attendees

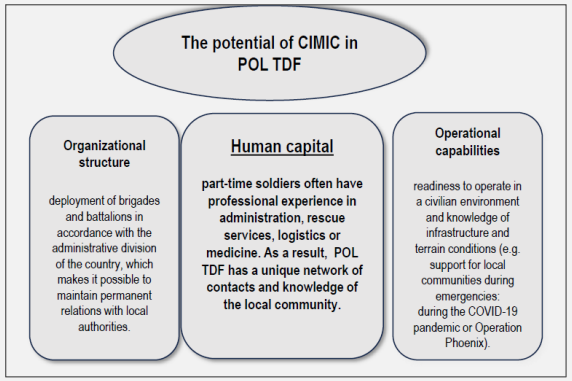
KEY INSIGHTS

Presentations Ministry of Defense (MON) and Territorial Defense Forces (TDF)

Insight

- On Wednesday morning, we were welcomed at an army base, about 45 minutes outside the center of Warsaw. In a specially erected tent, we were given three presentations by the Polish Ministry of Defense and the Territorial Defense Forces (TDF).
- The strength of the TDF lies in its local presence (Permanent Areas of Responsibility). Because brigades and battalions follow the country's administrative boundaries exactly, service personnel build deep trust and established lines of communication with local authorities, emergency services and civilians even before a crisis arises. Furthermore, the TDF consists largely of part-time soldiers who, in their daily lives, work in logistics, healthcare or public administration. This provides the armed forces with a unique and immediately deployable network of civilian expertise and local knowledge.
- The TDF operates a flexible support model. In peacetime and during crises, the TDF supports the civilian authorities (such as during the COVID pandemic, floods or border security operations). In wartime, its role shifts to combat tasks aimed at delaying the enemy, in close cooperation with the regular army.
- 'Education with the Army' in schools: The TDF organizes large-scale, hands-on training sessions in primary and secondary schools to teach children self-defense skills, crisis awareness and basic habits. This program had already reached over 160,000 pupils in 2024 and 2025.
- The setting made an immediate impression. Whilst the presentations were underway, gunfire could be heard constantly in the background, drones flew overhead and tanks drove past. The field exercises continued as normal, which made the urgency of the story palpable.
- In addition to the presentations, we were given a guided tour of the Eastern Shield (slide 21) and a 'Be Ready' training session (slide 22).

Impressions



KEY INSIGHTS

Guided tour Eastern Shield

Insights

- At the army base, we were given a guided tour of a replica section of Eastern Shield (Tarcza Wschód), the large-scale Polish program to reinforce the eastern border with Belarus and Russia using trenches, bunkers, anti-tank obstacles, barriers and detection systems.
- What struck the Vanguard most was how much this resembled warfare from the First World War, a true trench war. At the same time, there were undeniably modern elements. Anti-drone equipment had been installed throughout the trenches, such as loose iron chain-link fencing at every entrance to prevent drones from flying inside.
- The front line was just a few hundred meters: rows of concrete dragon's teeth (star-shaped anti-tank obstacles), fences and detection systems. According to the soldiers, landmines had been laid in the area in between. This is also evident from recent policy: together with the Baltic States and Finland, Poland withdrew from the Ottawa Convention on anti-personnel mines in July 2025.
- This firsthand view of the trenches left a deep impression and meant that we returned from Poland in low spirits and considerably less optimistic. It was a poignant experience to see just how tangible the preparations for a large-scale conflict are here.
- Both during this guided tour and from the ambassador's account, a stark message emerged: the sense that a conflict with Russia is inevitable. This raises the question of whether Dutch society ought not to be much more actively engaged with this reality in order to emphasize its urgency.

Impressions

KEY INSIGHTS

Be Ready-training (from the TDF)

Insights

- We were the first Dutch delegation ever to receive the ‘Be Ready’ training, which the Polish Territorial Defense Forces provide to civilians and businesses to help them become more resilient in times of crisis and war.
- The ‘Be Ready’ training courses offered to civilians are one-day, free of charge sessions for individuals and Vanguards, structured in a modular format. Civilians can choose from four specific 8-hour tracks: medical training, combat medicine, cyber security and survival.
- The training we received consisted of four parts: ensuring a safe supply of drinking water, making a fire, building a shelter and putting together an emergency rucksack.
- The experience was heightened by the fact that other exercises were taking place on the site at the same time: constant gunfire and drones flying overhead in the background.
- What stuck the most was that the Poles are not only well advanced in terms of the physical and logistical aspects of their civil resilience, but above all in their mindset. As they said: “Putting together an emergency kit isn’t difficult, but having a serious conversation about it with your loved ones is.”
- That mental aspect kept coming up. With the children’s backpack, it was about small things like toys, a cuddly toy and photos of loved ones. And when it came to making a fire: alongside all its practical value, the warmth and light offer, above all, mental support in times of crisis.
- The practical value of simple, pragmatic solutions was also emphasized by the instructors: “It’s not stupid if it works.”.
- In Poland, there is significant investment in the training and education of reservists and civilian first responders, as well as in the training and education of children in primary and secondary schools.

Impressions

GROUP TRAINING - DELIVERED IN PARALEL ACCORDING TO PARTICIPANT'S PREFERENCES			
MEDICAL TRAINING COURSE (8h)	COMBAT MEDICINE COURSE (8h)	CYBERSECURITY COURSE (8h)	SURVIVAL COURSE (8h)
• Elements of Basic Life Support; including CPR, the recovery position, first aid for wounds and injuries; • Calling for emergency medical services; • Using an automated external defibrillator (AED); • Fear management; • Personal hygiene.	• Types of combat injuries (amputations, gunshot wounds and blast injuries), • Practical application of tactical tourniquets and management of junctional bleedings, • Hemostatic dressings, • Prevention of post-traumatic hypothermia, pathology of blast and burn injuries, • Walking Blood Bank – directions for development.	• Mobile devices, • Data leak and phishing, • Passwords, two-factor authentication (2FA), paswordless login, • Resilience to misinformation (fake news). Informative lecture. Practical training. Case study. Checklists.	• Preparing yourself and your house for crisis situations; • Warning signals and how to behave after an alert is announced; • Responding to threats; • Handling basic firefighting equipment; • Public safety and order (including cooperation with emergency services).
OPTION TO CHOOSE THE TRAINING SUBJECT AREAS			

KEY INSIGHTS

Systemic collaboration

Insights

- On Wednesday afternoon, the program featured a session on ‘systemic collaboration’, led by systemic practitioner Siets Bakker. The aim was to step away from analytical thinking for a moment and look at what is happening beneath the surface. What happens when you approach complex issues with your emotions and body, rather than just with your head?
- The focus soon turned to the question of how, as a lead Vanguard member, you establish your position within your own organization and gain buy-in on these issues.
- Central to this was the relationship with the board members. Distance gives them the flexibility to step in and out, which some perceive as fragile. The key point: creating distance is not the same as stepping out. In the constellation, the space between the board member and the lead Vanguard member was large, but eye contact was maintained.
- The exercise revealed the multi-layered nature of the Vanguard: from the individual to the Vanguard, their own organization, the sector and, ultimately, the system.
- After a year and a half, there is no longer any doubt about the motives behind the parties’ involvement. Trust has grown and we are gaining a better and better understanding of how we can work together to take swift, concrete action.
- A second exercise centered on two questions: “What are you willing to contribute to this collaboration?” and “What are you not willing to contribute?”. This sparked a lively discussion about the role of the steering Vanguard and everyone’s individual role within it.
- One outcome of this systemic constellation is the realization that we need to share the knowledge and sense of urgency we have gained much more widely within our own organization, rather than keeping this solely within the lead Vanguard.

Impressions

3. Actions & follow-up

ACTIONS & FOLLOW-UP

During the work session on Thursday, 5 actions were identified

ACTIONS	WHO?
1. Disinformation	**Lead:** TNO **Team:** NVB, NIPV, VNG, ABN AMRO, KPN, Rabobank, Municipality of Rotterdam, Deloitte, AMS-IX
2. Resilient citizens based on the Polish model	**Lead:** Rode Kruis & Leger des Heils **Team:** JenV, KPN, NIPV, VNG, Municipality of Rotterdam, Safety region Noord-and Oost-Gelderland, Deloitte
3. Reservists and critical infrastructure	**Lead:** Port of Rotterdam & NS **Team:** JenV, Defense, VNO-NCW, KPN, TenneT, Gasunie, Deloitte
4. Putting it on the agenda, urgency & positive narrative	**Lead:** Eleonora Russell & WeerbaarNL **Team:** Rob Bauer, Deloitte, NIPV, VNG
5. Accelerating Resilient Stores	**Lead:** Albert Heijn **Team:** T.B.D.

Detailed ideas, actions and roles

1. Disinformation

Common thread:
- *There is a great sense of urgency; the Netherlands is falling behind.*
- *No clear leadership or central point of contact for disinformation in the Netherlands. That is where the opportunities lie.*
- *Various initiatives are already underway (including NIPV); the challenge is to ensure coherence, centralization and a strong role for public-private partnerships.*

Lead:
- *TNO*

Team:
- *NVB*
- *NIPV*
- *VNG*
- *ABN AMRO*
- *KPN*
- *Rabobank*
- *Municipality of Rotterdam*
- *Deloitte*
- *AMS-IX*

Actions:
- *TNO intends to develop an initial session, possibly as early as this summer.*
- *Plan: start by building up momentum with a smaller Vanguard, then roll it out widely with the entire Vanguard in September.*
- *Explain the scenario analysis during the directors' dinner (NVB).*
- *Develop and offer training courses based on the HackShield model, for example in schools (NIPV).*
- *Involve the Ministry of Economic Affairs and Climate Policy (EZK), the Ministry of the Interior and Kingdom Relations (BZK) and the National Coordinator for Security and Counter-Terrorism (NCTV) where possible.*
- *Investigate whether a rapidly responding 'trusted community' can also be set up within the Vanguard to tackle disinformation.*

2. Resilient citizens based on the Polish model

Common thread:
- *Resilience is also about the capacity of citizens themselves; Poland is a step ahead in this regard.*
- *Be Ready' is the Polish model: accessible, free of charge and widely available to citizens and businesses, with a choice of packages tailored to individual circumstances.*
- *Training focuses on personal resilience as well as the role people can play during crises.*
- *Programs can be delivered both centrally and through businesses; this reinforces each other and reaches the widest possible audience.*
- *Relieving the burden on the Ministry of Defense where possible: reservists within (Vanguard) organizations can lead training sessions.*

Lead
- *Rode Kruis*
- *Leger des Heils*

Team:
- *JenV*
- *KPN*
- *NIPV*
- *VNG*
- *Municipality of Rotterdam*
- *Safety region Noord-and Oost-Gelderland*
- *Deloitte*

Actions:
- *Develop a comprehensive training program for members of the public and businesses, based on the Polish model.*
- *Examine, on an organization-by-organization basis, how this can be developed and delivered internally, with in-house staff acting as trainers (for example: KPN has already entrusted this to its HR department).*
- *Accelerate and scale up existing 'Be Ready'-style training programs.*
- *Secure a commitment from each Vanguard organization, for example by registering a fixed number of employees.*

Detailed ideas, actions and roles

3. Reservists and critical infrastructure

Common thread:

- *Key concept: a separate Vanguard of 'vital infrastructure reservists' for each infrastructure organization, independent of the Ministry of Defense. In the event of war, the Ministry of Defense calls up its own reservists, who are therefore unavailable for vital infrastructure duties.*
- *Key task: maintaining critical functions.*
- *Strong link to Article 5: which critical entities does the Ministry of Defense protect in times of war? A difficult but necessary discussion, and the timing aligns with this strategic theme of the Vanguard.*

Lead

- *Port of Rotterdam*

Team:

- *JenV*
- *Defense*
- *VNO-NCW*
- *KPN*
- *TenneT*
- *Gasunie*
- *Deloitte*

Actions:

- *Initiate discussions with the Ministry of Infrastructure and Water Management (IenW), involving the Ministry of Justice and Security (JenV) if necessary (Bastiaan Walenkamp).*
- *Develop the plan in a smaller Vanguard, including a link to Article 5, before involving the wider steering Vanguard.*
- *Involve private security firms.*
- *Clarify what companies are already doing, learn from one another, and give managers a nudge.*
- *Make better use of the capacity of security organizations; explore the possibility of discussions with the trade association.*
- *Develop a legal framework (longer term).*

4. Putting it on the agenda, urgency & positive narrative

Common thread:

- *There needs to be a greater sense of urgency in the Netherlands. In Poland, it was plain to see that a conflict with Russia 'is going to happen'. We must dare to communicate more clearly and transparently on this issue.*
- *It is important that we continue to communicate about resilience in the broadest sense, not just war scenarios, but also large-scale crises.*
- *The Vanguard wants to offer a positive counter-narrative: to show what is possible and what the Vanguard is already doing, in order to inspire the silent majority to take action.*
- *A prerequisite for positive communication is that it is underpinned by concrete action.*
- *The Vanguard's role is that of a connector: linking individual initiatives and demonstrating coherence.*
- *Commitment from decision-makers is a prerequisite.*
- *Framing: focusing on sovereignty and autonomy.*

Lead

- *Eleonora Russell*
- *WeerbaarNL*

Team:

- *Rob Bauer*
- *Deloitte*
- *NIPV*
- *VNG*

Actions:

- *Inspire one another and use the directors' dinner to highlight who is responsible for what (lead Vanguard).*
- *Put it on the agenda and inspire others to raise the profile of the theme more strategically (Rob Bauer).*
- *Put the Article 5 scenario more explicitly on the Board of Directors' agenda (Bastiaan Walenkamp).*
- *Link ideas and actions to 1–2 directors or CEOs as sponsors, to secure support at the top.*
- *Put forward a positive counter-narrative that shows what is possible (Eleonora Russell).*

Detailed ideas, actions and roles

5. Accelerating Resilient Stores

Common thread:

- *Building on the ongoing project to make 1,000 shops resilient based on the Finnish model, allocated according to market share within the supermarket sector.*
- *Objective: shops that can remain operational in the event of, for example, a power cut.*
- *The Vanguard as a catalyst and a platform for requests for assistance.*
- *Ruud (AH) will provide further context and a more specific request for assistance during the lead Vanguard meeting in September.*

Lead:

- *Albert Heijn*

Team:

- *Request for help to the entire Vanguard*

Actions:

- *Put the 'resilient shops' concept on the map in collaboration with CBL and fellow supermarkets (AH). Select shops in proportion to their market share (AH).*
- *Arrange emergency power supply: mobile generators at shop locations in times of crisis, including dependencies such as fuel supply.*
- *Organize the necessary framework: security around shops and communication between shops, distribution centers and head offices.*
- *Collaborate with local authorities and safety regions to develop, test and implement the concept.*
- *Deploy a task force to respond to requests for assistance arising from the project, with a more specific request for assistance due around September (AH).*

Follow-up

ACTIES FOR THE VANGUARD:

- Implementing the identified actions through lead organizations from the learning journey
- Informing and mobilizing everyone's organizations
    - Sharing the program booklet and debrief with key stakeholders
    - Wider dissemination of ongoing and identified Vanguard actions
- Developing ongoing initiatives relating to the 72-hour power cut

ON THE AGENDA:

- 4 September: Vanguard meeting
- Eind of September: Directors meeting

4. Feedback

FEEDBACK

Reactions from participants on the learning journey to Poland

- **Growth and trust within the Vanguard**: It's remarkable to see how the Vanguard has grown since Finland. The trust within the Vanguard is particularly striking. This was evident not only in the discussions, walks and Q&As, but just as much in our interactions, the dinners and moments of relaxation. This underlines just how essential it is to continue organizing regular Vanguard meetings in person in the Netherlands as well: the study trip has proven that mutual trust and strong personal bonds are the driving force behind our collective drive.

- **Applying this to our own organizations**: It remains a challenge to explain to all Dutch organizations exactly what we experienced in Poland and just how special it was. Participants are looking for guidance and support to effectively convey this story within their own organizations.

- **Motivation to take action:** The Vanguard is highly motivated to continue working in the Netherlands and has returned with an impressive list of new initiatives and proposals. Key Vanguard members are proactive and willing to assist one another with requests for help. It was explicitly stated that we do not merely wish to launch new initiatives, but also want to inject extra energy into existing projects, scaling them up and accelerating their progress.

- **Organization, program and program booklet**: Our compliments on the organization and the program, it was an impressive trip. The Vanguard particularly appreciated the well-organized logistics and the fact that everything was taken care of for them. The program booklet was also highly appreciated, not only for the logistical details but also for the informative content, which ensured the participants were well prepared for the trip.

- **Clear objectives**: The precise wording of the objectives ensured a clear scope. Partly as a result of this, we succeeded in achieving all these goals.

- **Systemic session**: Siets Bakker's incisive and thought-provoking questions led to new and interesting discussions that are often not possible amidst the hustle and bustle of everyday life. In addition, there was also feedback for next time: some members of the lead Vanguard would have preferred a joint systemic constellation rather than smaller constellations in breakout sessions, and the concept of systemic work could have been introduced in slightly more detail beforehand to help the Vanguard engage even more fully with this working method.

- **Maintaining a sense of urgency**: We want to hold on to the sense of urgency we experienced in Poland and bring it back to our Dutch organizations. In the Netherlands, that sense of urgency is still too low.

- **Conveying the 'Polish spirit' within the organization**: The ingredients needed to convey the insights gained are in place, but it remains a major challenge to truly convey that compelling sense of urgency to our own colleagues in the Netherlands. Participants are actively seeking guidance and tools to ensure this complex and impactful message is effectively communicated within their own organizations.

- **Communication**: Members of the Vanguard are enthusiastic about the energy and attention being devoted to external communication. They highlight Anja's commitment: she wrote articles about the study trip whilst on the journey and provides a platform for the Vanguard on WeerbaarNL and express their confidence in Eleonora Russell's role as head of communications. These new forms of communication not only raise awareness and a sense of urgency in the Netherlands but also increase support within all affiliated organizations.

- **Room for new faces:** The Vanguard is constantly evolving, growing and, at times, changing in composition. Despite the busy program, we should have set aside more time to introduce the new faces at the start of the trip.

Appendix: Bibliography

BIBLIOGRAPHY

Documents, sources and in-depth literature

POLICY DOCUMENTS & REPORTS

- Cichy, H., & Krzemiński, B. (2026). *Jak holenderskie firmy współtworzą polską gospodarkę*. Polityka Insight.
- Government of Poland. (2023). *Narodowy Program Ochrony Infrastruktury Krytycznej*.
- Government of Poland. (2025). *Program Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 [National Population Protection and Civil Defense Program 2025]*.
- Rządowe Centrum Bezpieczeństwa (RCB). (2025). *Strategy on the resilience of critical entities - Standards for ensuring the proper operation of critical infrastructure: Best practices and recommendations*.

ONLINE ARTICLES (WEERBAARNL)

- Content manager WeerbaarNL. (2026, 3 juli). Welke lessen leren Nederlandse bedrijven van Polen op het gebied van veiligheid en weerbaarheid? WeerbaarNL.nl.
- Content manager WeerbaarNL. (2026, 22 juni). Warschau: waar weerbaarheid onderdeel van het heden én verleden is. WeerbaarNL.nl.
- Markus, J. (2026, 24 juni). Evolutie van Russische cyberoperaties tegen Polen: lessen voor overheid en bedrijfsleven. WeerbaarNL.nl.
- Markus, J. (2026, 25 juni). De strijd tegen desinformatie en hybride oorlogsvoering. WeerbaarNL.nl.

Thank you all for the learning journey, your insights and your cooperation!

If you have any questions and/or comments, please do not hesitate to contact:

Bastiaan Walenkamp

Secretary National Coalition for Security and Resilience

bwalenkamp@deloitte.nl