friends of europe

AUTUMN 2019

Leaders' response to hybrid threats: a real-time case study

REPORT

Cover image credits: Rost-9/Bigstock, p.8/3 CC Flickr - EU2016 NL

Friends of Europe's Peace, Security and Defence Programme is supported by the United States European Command (EUCOM). Our work is firmly anchored in our expertise in a range of fields, including energy and climate change, geopolitics, international development, migration and health. We seek a holistic approach to European, transatlantic and global security policies. Security considerations are, in turn, mainstreamed into these areas of expertise, enriching the debate by encouraging experts to think outside their comfort zones.

We are grateful to Facebook for their support for the exercise.

With the support of

EU2019.FI

Co-funded by the
Europe for Citizens Programme
of the European Union

Rapporteur: Paul Ames
Publisher: Geert Cami
Senior Fellow: Jamie Shea
Director of Programmes and Operations: Nathalie Furrer
Programme Managers: Elena Saenz Feehan, Antonia Erlandsson
Programme Assistant: Katherine Pye
Events Manager: Chris Irons
Photographer: Philippe Molitor
Editor: Arnaud Bodet
Design: Elza Lőw

We are very grateful to Chris Kremidas for his support in constructing the scenario and his inspiring can-do attitude.

Table of contents

Executive summary

This report draws attention on the urgency to improve cooperation between the public and the private sectors in order to increase readiness and resilience to hybrid challenges. It includes several recommendations based on the findings from Friends of Europe's tabletop simulation exercise 'Hybrid warfare readiness' where senior officials and experts from NATO, the EU, national authorities, the media and business were gathered to test their collective responsiveness to a range of credible hybrid threat scenarios.

Whereas NATO and the EU have already held exercises to deal with hybrid threat scenarios, the missing link has always been the private sector. Their involvement should not be neglected, as they own and operate a large percentage of the critical infrastructures being attacked. The novelty of Friends of Europe's tabletop simulation exercise was to bring private sector representatives together with national government NATO and the EU experts.

Based on the discussions and findings of this innovative simulation exercise, the report identifies ten recommendations to improve cooperation between the public and private sectors in order to deter, detect and defend societies from hybrid attacks.

1. Creating co-working arrangements for public-private partnerships

It is essential for the public and private sectors to cooperate quickly in a structural, rather than *ad hoc*, manner. This means building trust and creating a 'co-working' space where the private and public players can work as partners and formulate policy together. For this to happen, there should be regular joint training and exercises where public- and private-sector operatives learn to work better together.

2. Implementing assurances for public-private information exchange

Since businesses are often the first to spot emerging problems, information exchange networks should be created to allow two-way flows of early-warning data. Information-sharing and trust-building between the public and private sectors can be improved by putting proper assurances in place so that government bodies become trusted platforms for companies to share information without compromising sensitive business data. Governments and international organisations can also overcome reluctance to share classified information with private entities by establishing prior clearance arrangements

3. Establishing clearer roles for the EU and NATO in joint emergencies

More work is needed to define the role of both the EU and NATO in a shared emergency. Both NATO and the EU should work more with member governments to establish definitions of what type of hybrid activity would constitute an attack able to trigger responses under the North Atlantic Treaty or the EU's Lisbon Treaty mutual defence and solidarity clauses. Clear definitions are required for cases when a non-EU partner country could call for assistance from the Union, or when a country outside the Alliance could receive NATO support.

The two organisations should also establish a joint approach on how to deal with countries suspected, or revealed, to be behind hybrid activity. Beside structural ties that should be honed by regular meetings, training and exercises, personal contacts are important so that cyber and intelligence staff in both organisations and in national capitals are familiar with who they need to call in an emergency.

4. Enhancing intelligence though public-private cooperation

Intelligence needs to be improved in order to generate timely forensic and technical reports on who is behind hybrid action and provide a clear initial response. Enhanced cooperation with the private sector can be valuable, particularly in the rapid identification of culprits in cyberattacks.

5. Establishing clear guidelines on how to proceed once the perpetrator has been identified

Coherent approaches and clear guidelines on how to move forward once attribution has been determined need to be established, clarifying legal issues so that evidence of attribution can stand up in court.

6. Improving cooperation between the military and the private sector

Cooperation between the military and the private sector should be improved. The private sector is in the position to provide detailed information on critical infrastructures and technical expertise that could allow the authorities to better respond to the threat if military action is necessary.

7. Increasing cooperation between local and national police bodies at the EU and NATO level

Cooperation, training and emergency planning between police forces at European and NATO level should be intensified as most responses to hybrid threats currently fall well below the level of military involvement. The links within the EU and NATO need to be upgraded by training at the police and law enforcement levels.

8. Enhancing cooperation between the EU, NATO and individual government public affairs and communication teams

Given that it is essential that coherent messages are sent from NATO, the EU and individual allies/member states, cooperation between their public affairs and communication teams will need to be intensified. Pro-active communication is required to prevent the formation of an information vacuum that risks leaving the public confused and prone to panic, or of being exploited by hostile elements. That requires acting fast and filling the information void early to promote a sense of confidence that reassures and unites society.

9. Increasing investment and cooperation for counter-disinformation initiatives

More investments in efforts to tackle disinformation campaigns are needed. And in the case of deepfake technology, private sector cooperation could prove useful in providing the technical expertise required to prove a video is faked.

10. Building whole-of-society resilience

As hybrid attacks target the core of our democracies, building whole-of-society resilience is essential for defence and deterrence. To do so, authorities should put more effort in raising citizens' awareness of the nature these threats and give advice to citizens on how to prepare for terror and cyberattacks, natural disasters, serious accidents, military conflicts and other extreme situations.

The EU, NATO and national governments need to work with local governments to bring in citizens and the private sector to plan ahead, prepare, and practice together in order to be ready together. Governments have to be prepared to invest more in resilience and make sure their communities and businesses can deal with interruptions and bounce back quickly.

Context

Since Russia's aggression in Ukraine in 2014, which led to the illegal annexation of Crimea and occupation and conflict in the east of the country, the West has stepped up its response to the threat of hybrid attacks. However, there is a widespread recognition that much more needs to be done so that NATO and the European Union can provide timely, joined-up approaches to hybrid challenges. Those responses need to bring in civil and military players, link up national authorities with international organisations and unite the public and private sectors in a whole-of-society approach to prepare for, deter and defend against hybrid threats.

That was the background of a unique exercise organised by Friends of Europe that gathered senior officials and experts from NATO, the EU, national authorities, the media and business. The goal was to test their collective responsiveness to a range of credible threat scenarios. NATO and EU nations were challenged by a cascading series of threatening incidents against a background of heightened tensions with a large, hostile neighbour to the east.

Whereas NATO and the EU have already held exercises to deal with hybrid warfare scenarios, the missing link has been the private sector which owns and operates a large percentage of the critical infrastructures being attacked. The novelty of Friends of Europe's tabletop exercise was to bring private sector representatives together with national government NATO and the EU experts. This facilitated a more realistic and comprehensive review of how Western democracies would deal with hybrid attacks.

With each episode, teams were given 45 minutes to react to the events. Groups were asked to consider EU-NATO coordination, private and public sector action, as well as the strategic communication and public affairs response. The aim was to analyse, in real-time, the nature of the threat; establish their level of situational awareness; agree on procedures; decide who takes the lead; and examine what measures each player has in its toolbox to deal with both the immediate emergency and longer-term challenges thrown up by the crisis.

From there, the exercise enabled participants to identify shortfalls in hybrid response capabilities, gaps in how key actors communicate and collaborate, and how more resilience can be built into Western systems to deter hostile powers from launching hybrid attacks.

Participants emphasised the need for better intelligence sharing to ensure that relevant policymakers are fully informed of hybrid risks; the importance of greater international cooperation between law-enforcement and civil protection services to match that already established among military organisations; for pro-active media strategies to keep citizens informed and debunk fake news during a crisis; and outreach to all sectors of society to counter adversaries' efforts to undermine faith in democratic institutions. Above all, participants stressed the importance of better communication and cooperation between NATO and the EU and the need for integrated structures and procedures to cement an effective, real-time cooperation between the private and state sectors to prevent, deter and defend against cyber and other hybrid threats.

Nature of the threat

Hybrid threats take multiple forms, from election interference to covert use of force, cyberattacks to targeted assassinations, fake news to economic sanctions, exporting crime and corruption to fomenting unrest and support for violent proxy groups.

While its latest manifestations exploit technology and weaknesses in modern, open societies, its aim is age-old. One participant noted that it was already present in the 6th century BC objectives laid out by Chinese strategist Sun Tzu to achieve military success without using military force. In today's context that is particularly true of adversaries who cannot match NATO's military strength but have managed to put the West on the back foot through the aggressive use of hybrid tactics.

"The objective is to undermine faith in democracy," explained one exercise contributor. "They are trying to impinge on what is dearest to us, which is our democracy, governance, rule of law, human rights," said another. "It's been devised by intelligent people on the other side who have analysed our strengths and weaknesses; and have taken advantage of our weaknesses while isolating themselves from our strengths," added a senior military official.

Several participants made the point that hybrid war is the new real war, seeking to do deep harm to our societies and structures. They stressed that it is not an abstract concept or distant threat, but rather a real challenge faced on a daily basis by Allied security forces. This has taken the form of incessant cyberattacks to political interference seeking to undermine democratic values, media campaigns, probing of military defences, or actual attacks such as the use of chemical weapons by Russia against targeted civilians in Salisbury. One senior government official said Russian cyberattacks on his country were "a never-ending story."

Faced with the real damage being done by such tactics and the risk that cyberattacks could be used to soften up democracies before the launch of a kinetic attack, there was consensus that the West urgently needs to step up its defences and close "the gap between the threat, which is continuing to grow, and the preparation."

Aims of the exercise

With that in mind, the day-long tabletop exercise was a welcomed opportunity to pool expertise from the public and private sectors. They tackled realistic scenarios which created deep crises for Europe and NATO without a shot being fired. The goal was to boost cross-sector and cross-institution cooperation, look for weaknesses within response procedures and find ways to fix them.

By building up societal resilience and adequate preparation and defence measures, it should be possible to deter adversaries from pursuing hybrid action in the same way as NATO's mutual defence guarantee deters open military attack. "How do we get inside their calculus to convince them it's not worth it?" asked a defence specialist from one Allied nation. "I believe it can be done."

Meanwhile, a denial-of-service attack has hit a bank in Erlandia. The institution has links to the family of a leading opposition politician who aims to take the country into NATO if she wins upcoming elections. Heightening unease were reported sightings of a submarine in Erlandian waters and suspicious fishing boats with diving equipment off the coast of Huertaland.

The second round saw another emergency in Huertaland with a criminal syndicate calling itself the Shea Liberation Front (SLF) hacking into the controls of a ship carrying Liquified Natural Gas (LNG) and threatening to explode it, possibly in or near another of the country's seaports. Authorities were given six hours to pay €30mn into a Cayman Island bank account to avoid the attack.

Meanwhile, the fire at Huertaland's other port has been declared accidental. Tensions are exacerbated by the Camiland media circulating a deep-fake video purporting to show NATO's Secretary-General plotting with the President of Oksania to retake the territory of Kremmydia which was seized by Camiland from Oksania in 2019. Although NATO denies the veracity of the video, Camiland put its forces on high alert and sent more troops to Kremmydia.

Finally, an undersea cable linking Erlandia to mainland Europe has stopped functioning. That severely restricts financial, data and voice communications and causes disruption in European markets. Erlandia believes the cable has been deliberately cut or jammed. The government proposes postponing the elections until the crisis is resolved. Camiland offers Erlandia the use of its data pipelines while repairs take place.

"These scenarios are not science fiction, everything has either happened already or is possible with today's technology," one of the organisers explained before the group split into three to look at managing the crises from the point of view of NATO and the EU; national governments and private business; and strategic communications and public affairs. The 45-minute response time given each group showed that there are effective tools available to react to the fast-moving emergency, even when the situation is complicated by neither of the two affected countries being members of both the EU and NATO.

A graduated response would see an increased intelligence focus on the crisis and greater sharing of information between national governments, the EU and NATO. Meetings of the EU Council and NATO's North Atlantic Council could be called to show support for the beleaguered nations and plan the response.

Outreach to the private sector could be particularly important in securing details of the hijacked ship. It could also provide alternatives for the damaged cable or prove the contentious video as a fake.

The EU could activate its disaster response procedures to help cope with the fire and potential impact of the ship exploding, and deploy resources to mitigate the financial impact of the disconnected cable. As tensions escalated, NATO could show support by beginning to plan for the preventative deployment of military units to the region. In the last resort, military action might be needed to take out the rogue ship.

One key problem in dealing with hybrid action is understanding that an attack is taking place and discovering who is responsible. "When do we understand that this is an attack?" asked a former senior government official. "That's a key problem. When do you know you are in an emergency," they added. "If (an ally) is invaded by military means, we know what to do, but with this we don't really know. There is a crisis, but whose crisis is it?" The exercise scenarios would test responses and help find the answer to those questions.

The scenario

The participants were given a three-stage scenario involving an escalating and multifaceted crisis affecting two fictional European democracies under pressure from a large, hostile power. Set in 2024, the scenario was centred on Erlandia, a member of the EU but not of NATO, and Huertaland, a NATO ally that is not an EU member. The two share a joint maritime border and both have land and sea borders with Camiland, a large Eurasian power that has historically had difficult relations with its neighbours and antagonistic dealings with the EU and NATO.
In the first scenario, Huertaland suffers a mysterious fire at a strategic seaport and a cyberattack that forces a shutdown of the electricity grid in a region with a significant Cami minority. That leads to claims of mistreatment by Camiland media. Tensions are already high after recent NATO exercises near an artificial island which Camiland is building to reinforce its claim to potentially gas-rich waters disputed with Huertaland.

1. **Kimmo Kohvakka**, Director General for Rescue Services at the Ministry of the Interior for Finland's representative to NATO's Civil Emergency Planning Committee in DG format and Simona Autolitano, Cybersecurity Strategist at Microsoft
2. **Merle Maigre**, Executive Vice President for Government Relations at Cybexer
3. **Despina Spanou**, Director for Digital Society, Trust and Cybersecurity at the European Commission Directorate General for Communications Networks, Content & Technology
4. **Burcu San**, Director of Operations at NATO and **Jaap de Hoop Scheffer**, Trustee of Friends of Europe, Former NATO secretary general and former Dutch minister of foreign affairs (2002-2003), Pieter Kooijmans Chair for Peace, Law and Security at Leiden University

Conclusions and recommendations

Despite those active responses, the exercise also pointed to the need for improvements to close gaps in counter-hybrid capabilities.

The private sector

The need to ensure that public and private sectors can cooperate quickly in a structural rather than ad hoc manner was one of the key messages to emerge. "We have to have the public and private sectors together, usually there is quite a gap," said one experienced decision-maker. "The private sector should be an absolutely essential partner."

> "Efforts should be made to support (and in some instances require) businesses to prepare for unexpected shocks to the critical infrastructure and to the supply lines on which they depend. They should also be encouraged to work together, so that they are better able to recover from some traumatic event. It must be the duty of Governments (and cross-national institutions) to ensure that critical infrastructure is made more resilient, that the right regulatory environment to facilitate this is created, and that there is adequate investment in essential services

Jonathan Toby Harris, Member of the House of Lords National Security Strategy Joint Committee in the United Kingdom

Partnership was the key word. Participants stressed the need to build trust that creates a "co-working" space for private and public players to ensure seamless cooperation in the event of a crisis. "Partnership with the private sector has to be more than just cooperation," said an official from one NATO ally. "It should be about formulating policy together, not just cooperating when you have a problem," they added, pointing out that the private sector is often the target of hybrid attacks as well as a provider of solutions.

To bring about that level of cooperation, there should be regular joint training and exercises where public- and private-sector operatives can work together. Private-sector experts should be brought into policy-setting forums with national government and international organisations to discuss issues like cyber defences, protection of critical infrastructure and crisis management.

Since businesses are often the first to spot emerging problems, information exchange networks should be created to allow two-way flows of early-warning data. Mechanisms could be created to have private-sector representatives present both in routine security discussions and in government emergency response meetings. Tech companies could team up with government agencies to routinely provide analytical data on evolving incidents.

One example that was highlighted is the Estonian Defence League's Cyber Unit, which is mostly made up of volunteer IT professionals from the private sector, and functions like a "cyber national guard" to defend the country's public and private telecommunications sector. This was established after a severe Russian attack in 2007. "It works as a strong deterrence [and] raises the resilience of the country," said one participant.

A number of elements in the exercise scenario highlighted areas where private-sector participation could be essential in providing a rapid positive outcome to threatening incidents. Working with shipping companies, port authorities and tech experts could deliver essential information on the hijacked ship, facilitating a counter-hack or boarding to regain control.

This said, the shipping incident also revealed differences in approach between private and public actors, with business representatives generally in favour of paying the ransom which could probably be recuperated through insurance, while government officials were opposed to giving-in to terrorist blackmail.

> "As cyberattacks take place, [...] public-private cooperation is key to solve the immediate crisis and go back to normal. In order for this to happen, we should build upon existing arrangements such as the NIS Cooperation Group created with the NIS Directive. This Group could represent an initial way to materialize public-private cooperation and information sharing in case of a cyber incident or attack. On the other hand, we can and should also proactively promote a more peaceful and secure internet for people everywhere. Peace in cyberspace is something that both public and private sector want to achieve. The 'Paris Call for Trust and Security in Cyberspace' launched last year by the French government at the Paris Peace Forum represents a great starting point to achieve this. It is now time to act all together and implement those 9 principles we agreed on

Simona Autolitano, Cybersecurity Strategist at Microsoft

Private companies' tech expertise could prove essential in quickly unmasking the video as a fake, and media appearances from the tech industry would add credibility to efforts to persuade the public that the video is bogus. Likewise, private companies would probably be best placed to fix the severed undersea cable and to provide emergency communication alternatives while it is being repaired.

Both the public and private sectors need to be more aware of the risk of cyberattack and should exchange best practice on how to build better defences. In companies, cyber defence needs to be mainstreamed at executive level, not handed down to IT departments. More needs to be invested in situational awareness, prevention and recovery from attack.

> "There are significant costs involved in protecting against cyber-attacks. There is an additional cost associated with the implementation of sharing platforms, the exchange of intelligence and in participating in joint exercises and training. Large companies will make a trade-off between investing time and resources in some key government relationships and exercises, whilst small companies may not even have the resources to participate. In order for the recommendations to work, government and industry have to focus on establishing cost efficient, effective, sharing mechanisms. It requires a trusted platform for the exchange of sensitive information based on open standards (like STIX, TAXII, CybOX etc) with a low (cost and legal) barrier to entry

Leendert van Bochoven, Global Lead for National Security and NATO at IBM

"Cyber is not a technical issue, but a military and strategic issue," said one speaker. That investment should include subsidising or incentivising a more rapid turnover of computers and software to keep defences up to date in both private and state institutions, said one technology company representative. Both also need to give more value to tech staff, including by bringing in younger people who are often more aware of the latest technological advances.

Trust is essential in establishing operational exchanges both within the private sector and between companies and government. Business representatives expressed concerns that exchanging sensitive information could compromise competitive positions, harm their brand or lead to sanctions from other governments. "The private sector wants assurances that government will protect them, not share their information, that it stays confidential both ways," said one national defence expert.

A representative from a leading technology company explained that it needs to seek legal advice to check if it violates regulations by sharing information with security services. "If information gets out to media, it could have repercussions for the brand or affect customer confidentiality," they added, calling for guarantees that information handed to government will be treated as classified. Another speaker from the business world suggested that, with proper assurances in place, government bodies can become trusted platforms for companies to share information without compromising sensitive business data. They added that such exchanges were already happening in their sector.

Trust issues also need to be addressed from the other side, so governments and international organisations can overcome reluctance to share classified information with private entities. NATO is already working to solve that problem with a plan to grant necessary security clearance to dedicated industry people, said one official.

One particular factor that risks hindering public-private security cooperation is foreign ownership of essential infrastructure. "We've outsourced too much critical infrastructure to foreign players," said one participant. From banks to railways to power and telecoms networks, strategic institutions are often now in foreign hands. Officials said that complicates communication even when the companies concerned are from allied nations. With Chinese companies now controlling significant infrastructure across much of Europe, the problem runs deeper.

EU and NATO cooperation

Cooperation between the EU and NATO was another key factor highlighted by the exercise. Although it is clear significant progress has been made in boosting ties and putting in place structures and procedures to ease cooperation, much more needs to be done. NATO officials participating in the event said they had developed close contact with colleagues at the EU's External Action Service (EEAS) but were pleased and surprised to discover security-related work done within various directorates of the European Commission.

The nature of the exercise involving one country in NATO but not the EU, and the other in the EU but not NATO, gave some clear indications of which organisation needed to take the lead. More work is needed to define the role both take in a shared emergency. Clear definitions are required for cases when a non-EU partner country could call for assistance from the Union, or when a country outside the Alliance could receive NATO support.

Participants underscored the need for better strategic contacts between the two that need to be nurtured regularly. Connections must already be in place to ensure a smooth reaction in the event of a crisis. Beside structural ties that should be honed by regular meetings, training and exercises, personal contacts are important so that cyber and intelligence staff at both organisations and in national capitals are familiar with who they need to call in an emergency.

While stressing the value of multilateral approaches, participants recognised the primary role of national governments to call for assistance under the EU treaty or Articles 4 and 5 of the North Atlantic Treaty.

As the scenarios intensified, it was clear throughout that the governments of Huertaland and Erlandia had first responsibility for making key calls, such as on public announcements of attribution related to the incidents or calling for help from their allies. However, both NATO, the EU and individual allies should keep them fully informed with intelligence and make clear what options are available under their solidarity mechanisms, as well as sharpening readiness to respond if requested.

Participants suggested both NATO and the EU should work more with member governments to establish definitions of what type of hybrid activity would constitute an attack able to trigger responses under the North Atlantic Treaty or the EU's Lisbon Treaty mutual defence and solidarity clauses.

NATO and the EU should also ensure they are able to produce united messaging in a crisis, with procedures in place to cross check consistent media releases. The two organisations should also agree a joint approach on how to deal with the country suspected, or revealed, to be behind the hybrid activity. However, the exercise revealed divergent views on the level of dialogue that should be maintained with Camiland as the crisis scenarios played out.

Attribution

The question of attribution raised several issues on both a technical and political level. Contributors complained that intelligence needs to be improved in order to get timely forensic and technical reports on who is behind hybrid action, or even if suspect incidents are really malicious – the discovery that the fire in Huertaland's port was accidental served as a reminder of the need for caution.

In particular, the importance of prompt intelligence-sharing among Allied nations and with NATO and EU headquarters was emphasised. "There is a need for intelligence to prove a clear initial response," said one military expert. Here too, enhanced cooperation with the private sector can be valuable, particularly in the rapid discovery of culprits in cyberattacks.

> "Government actors still do not seem to realize the role the private sector can play in providing assistance on intelligence, especially early in hybrid situations. Currently, the "nervous systems" of each state extend only into the organs of state - not into the private entities which will be the first targets of a hybrid attack. Thus, the further development of public-private information sharing, to include new legal frameworks to enable it, are vital in bridging this gap
>
> **Chris Kremidas Courtney**, Multilateral Engagement Coordinator at the US European Command (EUCOM), Germany

Once attribution has been determined, the question of when to go public with the accusation was recognised as politically sensitive. "There is a huge political dimension to the attribution debate," acknowledged one senior former official. Concern that public finger-pointing could escalate tensions at a time of crisis was seen as a major concern. There were calls for a coherent approach and clear guidelines on how to move forward. This is difficult given different sensitivities among NATO allies and EU member states on the issue. Legal issues also need to be clarified, so that charges of attribution can stand up in court. However, one official pointed out that without attribution, it's impossible to deploy important deterrence tools, such as sanctions.

Ultimately, the question of whether to publicly unmask hybrid attackers rests with the individual nation under attack, although they should do so in consultation with allies. Where NATO or the EU are themselves targeted – such as in the case of the deep-fake video featuring the Alliance's Secretary General – procedures should be put in place to reach a timely agreement on when to go public.

It was pointed out that authorities will face mounting media and public pressure for clarity on whether an incident was malicious and who is behind it. Thus, the dangers of escalation have to be balanced with the need to keep citizens informed. The media can also be useful in providing bottom-up attribution, perhaps with help from judicious leaks where it has been decided not to make an on-the-record announcement of who is responsible.

Several participants noted that attribution should be a secondary requirement when resources need to be directed first of all at "putting out the fire" caused by the hybrid action.

Civil-military cooperation

Questions were raised over the nature of cooperation between military and civil capabilities, most notably by the exercise scenario involving the hijacked LNG tanker. Military experts agreed that, if other options failed, an armed attack "to take the ship out" would be needed to prevent it from being exploded in the port, thus causing severe humanitarian, environmental and strategic damage.
Given the short timeframe, there would be no time for NATO or the EU as organisations to mobilise military support for Huertaland. The first course of action would then be to seek bilateral support from allies, should the situation not be manageable unilaterally.

Cooperation with civil maritime authorities and the private sector could mean a military air or missile strike might be averted if they were able to provide detailed information on the ship or technical expertise that could allow the authorities to retake control – either through cyber countermeasures or a boarding. Cooperation between Computer Emergency Response Teams could facilitate such a solution.

The EU could prepare civil emergency backup, if requested by Huertaland, regardless of its lack of member state status. If called in early enough, that would allow the EU to provide quick and effective emergency civil protection and humanitarian aid should the incident escalate. It was recalled that the EU has a number of emergency instruments that can be mobilised within hours, to provide financial, civil protection and technical support. Communications could be improved to better coordinate the use of such instruments with military actions, including any taken by NATO.

A number of participants called for an intensification of cooperation, training and emergency planning between police forces at European and NATO level. They pointed out that such work currently falls well below the level of military cooperation, yet could be crucial to providing responses to hybrid threats. "We need to upgrade links within the EU and NATO, it's working with the military, but not with the police," said one expert. "You need to train, train, train."

Enhancing cooperation between the EU, NATO and individual government public affairs and communication teams

Media representatives stated that, in today's fragmented media landscape, neither governments, international organisations nor traditional media could hope to control the narrative in such crisis situations. "The narrative is inherently out of control," one said.

Given this challenge, it is essential that coherent messages are sent from both NATO, the EU and individual allies/member states. That means heightened cooperation between their public affairs and communication teams, something that already worked successfully during the Ukraine crisis in 2014, one official said. Meetings of the North Atlantic Council and the EU's Political and Security Committee (NAC-PSC) could help streamline press messaging and ensure both organisations present a united picture.

Pro-active communication is required to prevent the formation of an information vacuum that risks leaving the public confused and prone to panic, or of being exploited by hostile elements. That requires acting fast even before full facts are available. "Authorities need to fill the news space; they need to be agile in public messaging," said an official from one Allied nation. "You've got to be filling the void early."

> "Deliberate falsehood within the media needs to be legislated against and penalised heavily. Right now, it is only subject to civil liability excepting cases of defamation. Deliberate distribution of fraudulent information needs to be criminalised based on intent by Regulation within the EU
>
> **Kostas Dervenis**, Cybersecurity expert, corporate professional and author

Communications should promote a sense of confidence to reassure and unite society, added another. Choosing the right communicators to get across trusted and reassuring messages is important, with uniformed officials and private sector experts mentioned as good choices. Contributors warned that efforts to impose a news blackout or to cover up the nature of events were likely to backfire – especially given the speed with which news travels on digital platforms.

There was praise for the EU's East StratCom Task Force, set up in 2015 to tackle Russia disinformation campaigns. This effort was recently expanded to cover the western Balkans and the EU's southern neighbourhood. More investments in such efforts were urged. Counter-disinformation campaigns could increase outreach and support to independent media in hostile and sensitive countries; boost media education and awareness; develop rapid alert systems; coordinate resources; and facilitate the sharing of information and best practices. Participants were told that the incoming European Commission is supportive of such efforts.

Such resources could be useful in rebutting the deep-fake elements of the exercise scenario, using EU tools to track the origin of the fake and to provide truthful reporting to counter it. Using trusted journalists within hostile states would help. Private sector cooperation could also prove useful in providing the technical services required to prove the video was faked. However, indulging in similar "dirty tricks" to discredit the other side was ruled out. "We can't really play them at their own game," said one contributor.

The involvement of NATO in any crisis was seen as an escalation risk factor, given that the media would immediately equate the Alliance's involvement as a militarization of the situation. Therefore, NATO action should be balanced against de-escalation needs.

Given the influence of social-media platforms, a number of participants raised the question of regulation. "We need to have the social media companies at the table to see to what extent they are accountable for what they are doing," said one official. It was suggested that more social media players should be invited to attend future such exercises.

Building whole-of-society resilience

Ultimately, hybrid attacks target the core of democracies, so building whole-of-society resilience is essential for defence and deterrence. That includes raising citizens' awareness of the nature of the treat. "We have to do more than we have until now to make civil society aware of what is going on," said a senior participant. "If civil society cannot see what is fake and what is real, then: 'Houston we have a huge problem'."

The group was informed that NATO's post-2014 strategy to prepare, deter and defend against hybrid actions of the type unleashed by Russia against Ukraine had made good progress in building up preparations. However, much work remains to be done on deterrence and defence.

It is essential to bring in citizens. "If communities are not resilient, there is very little that governments can do, even with the involvement of the private sector," said one expert, adding that the failure to build robust societal responsiveness can have serious implications for military defences. "A nation that is not resilient cannot give military support in a crisis," they added.

Efforts by Nordic countries to build resilience were highlighted as good practice, such as the pamphlet "If Crisis or War Comes," distributed to 4.7mn homes in Sweden in 2018. It offered advice to citizens on how to prepare for terror and cyberattacks, natural disasters, serious accidents, military conflicts and other extreme situations.

> "We need to develop a four-fold approach to developing societal resilience. First, all Governments need to make their individual citizens and their households more resilient with a programme of information and encouragement to enable them to be able to withstand a major shock or infrastructure to the critical infrastructure on which they depend. This should be coupled with strengthening education programmes to make citizens more discerning about the information they receive and better able to detect and reject fake news, conspiracy theories and the like. Second, there is a need to strengthen the resilience of local communities, encouraging people to look out for and support their neighbours (particularly the most vulnerable)
>
> **Jonathan Toby Harris**, Member of the House of Lords National Security Strategy Joint Committee in the United Kingdom

Participants also heard how Finland's security forces work with local government and the private sector around the country. "We have to co-work together. No one has the possibility to have any approach other than to have the whole of society working together," said one Nordic country official. "We have to plan ahead together; we have to prepare together; we have to practice together in order to be ready together."

One private sector contributor pointed out that resilience has a cost and that governments have to be prepared to invest more "because the cost of not having resilience is even higher." As an example, another participant pointed to the disrupted undersea cable scenario as showing where investment could have boosted resilience by ensuring that alternative communications infrastructure was in place. "Most citizens are not prepared if there was a major interruption of their infrastructure," they said. "Make sure your communities and businesses have thought and thought and can deal with interruptions and bounce back."

Recommendations for future exercises included bringing in more top-level officials, more private sector representatives and social media experts into the mix. Other suggestions included varying the scenarios to provide a greater variety of threats and perhaps having a 'red team' as a responsive adversary.

"We have to be able to prepare; we have to be able to deter; and we have to be able to defend," a senior Western official said in summary. "If we adopt resilience it will serve us for all sorts of scenarios, so it's a win-win situation."

1. **Edoardo Camilli**, CEO of Hozint and European Young Leader (EYL40), **Johannes Luchner**, Director for Emergency Management at DG ECHO and **Leendert van Bochoven.** Global Lead for National Security and NATO for IBM Belgium
2. **Pauline Neville-Jones**, Member of the House of the Lords National Security Strategy Joint Committee and former minister of state in the UK, **Espen Barth Eide**, Former minister of foreign affairs, former minister of defence, Norway
3. **Jamie Shea**, Senior Fellow at Friends of Europe and former Deputy Assistant Secretary General for Emerging Security Challenges at NATO and **Stefanie Babst**, Head of the Strategic Analysis Capability at the Emerging Security Challenges Division (ESCD) of NATO

List of participants

Ioannis Askoxylakis
Cybersecurity Policy Officer at the European Commission, Directorate General for Communications Networks, Content & Technology

Simona Autolitano
Cybersecurity Strategist at Microsoft

Stefanie Babst
Head of the Strategic Analysis Capability at the Emerging Security Challenges Division (ESCD) of the North Atlantic Treaty Organization (NATO)

Jean Backhus
Hybrid Threats Officer at the International Military Staff (IMS) of the North Atlantic Treaty Organization (NATO)

Knud Bartels
Former chairman of the North Atlantic Treaty Organization (NATO) Military Committee (MC) and former chief of defence of the Kingdom of Denmark

Geert Cami
Co-Founder and Secretary General of the Friends of Europe

Edoardo Camilli
CEO and Co-Founder of Hozint—Horizon Intelligence and 2017 European Young Leader

Gudrun Carlsson
Senior Advisor International Affairs at the NATO-coordination- Secretariat for EU and International Coordination of the Swedish Civil Contingencies Agency

Piers Cazalet
Deputy Spokesperson at the North Atlantic Treaty Organization (NATO)

Pierre Cleostrate
Senior Expert at the Secretariat of the Task Force on Security Union at the European Commission Directorate General for Migration and Home Affairs

Jean-Louis Colson
Head of Unit for Transports Networks at the European Commission Directorate General for Mobility and Transport

Jonathan Comfort
Threat Investigator at the Threat Discovery Team, Facebook

Jaap de Hoop Scheffer
Trustee of Friends of Europe, Former NATO secretary-general and former Dutch minister of foreign affairs (2002-2003), Pieter Kooijmans Chair for Peace, Law and Security at Leiden University, President of the Dutch Advisory Council on International Affairs

Kostas Dervenis
Cybersecurity expert, corporate professional and author

Espen Barth Eide
Former minister of foreign affairs, former minister of defence, First Vice-Chair of the Standing Committee on Energy and the Environment for the National Parliament of the Kingdom of Norway

Christian Fjader
Director for Policy and Planning at the National Emergency Supply Agency for Finland

Paul Geehreng
Defense Policy Advisor at the US Mission to the North Atlantic Treaty Organization (NATO)

Axel Hagelstam
Counsellor for Civil Emergency Planning at the Permanent Representation of Finland to the EU

Vilmos Hamikus
Head of Hybrid Threats at the Service of Deputy Secretary General CSDP and crisis response of the European External Action Service (EEAS)

Jonathan Toby Harris
Member of the House of Lords National Security Strategy Joint Committee in the United Kingdom

William Holbrook
Security Lead of BT Group

Jimmy Jaber Bringas
Chairman of UniportBilbao and Co-founder and CEO of Sparber Group

Khan Jahier
Lead resilience staff officer at the Enablement & Resilience Section at the Defence Policy and Planning Division (DPP) for the North Atlantic Treaty Organization (NATO)

Chris Kremidas Courtney
Multilateral Engagement Coordinator at the US European Command (EUCOM), Germany

Kimmo Kohvakka
Director General for Rescue Services at the Ministry of the Interior for Finland's representative to NATO's Civil Emergency Planning Committee in DG format

Paul Leonhardt
Member of Steering Group Strategic Communication for the Federal Foreign Office in Germany

Johannes Luchner
Director for Emergency Management at the European Commission Directorate General for Humanitarian Aid and Civil Protection (ECHO)

Merle Maigre
Executive Vice President for Government Relations at Cybexer

Natasa Marvin
Member of the Rapid Alert System network, Slovenia Government Communication Office

Jan Meuris
Security Analyst at the Antwerp Port Authority

Tom Monballiu
International Community Relations Manager at the Antwerp Port Authority

Chris Muyldermans
Head of Policy Advice & Regulatory Affairs, KBC Group

Pauline Neville-Jones
Member of the House of the Lords National Security Strategy Joint Committee and former minister of state in the United Kingdom

Konstantinos Ntantinos
Policy & Communications Officer at the at the European Commission Directorate General for Communications Networks, Content & Technology

Rando Paurson
Counsellor of the Crisis Management Department at the Ministry of Economic Affairs and Communications for Estonia

Carl Peersman
Civilian Military Advisor (CIVAD) at the North Atlantic Treaty Organization (NATO) Supreme Headquarters Allied Powers Europe (SHAPE)

Inge Poelemans
Disinformation Outreach Officer at the European External Action Service (EEAS) Inter-institutional relations, policy coordination and public diplomacy

Vira Ratsiborynska
Research analyst at the North Atlantic Treaty Organization (NATO) Strategic Communication Centre of Excellence

Burcu San
Director for Operations at the North Atlantic Treaty Organization (NATO) Operations Division (OPS)

Robert Piotr Soltyk
Adviser at the European Commission Directorate General for Communication

Despina Spanou
Director for Digital Society, Trust and Cybersecurity at the European Commission Directorate General for Communications Networks, Content & Technology

Jamie Shea
Senior Fellow at Friends of Europe and former deputy assistant secretary-general at NATO

Paul Taylor
Senior Fellow at Friends of Europe and Contributing Editor for Politico

Leendert van Bochoven
Global Lead for National Security and NATO for IBM Belgium

Friends of Europe
Connect. Debate. Change.

+32 2 893 98 23
info@friendsofeurope.org
friendsofeurope.org

Friends of Europe is a leading think-tank that connects people, stimulates debate and triggers change to create a more inclusive, sustainable and forward-looking Europe.