friends of europe

SUMMER 2021

Testing resilience to hybrid threats: a real-time case study

REPORT

Cover image credits: Rost-9/Bigstock

Friends of Europe's Peace, Security and Defence programme aims to make sense of the emerging new geopolitical environment by analysing ongoing transnational challenges. To do so, we cover topics including the state of the EU's security and defence evolution, the transatlantic security partnership, peace and stability in the EU's neighbouring regions, the link between space, defence and security, the impact of increased digitization and emerging technologies on resilience, the integration of women into peace and security practices, the impact of conflict, and the value of peacebuilding initiatives.

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

With the support of:

2021PORTUGAL.EU

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

Publisher: Geert Cami
Senior Fellows: Jamie Shea & Chris Kremidas
Director: Dharmendra Kanani
Programme Manager: Elena Saenz Feehan
Programme Executive: Alex O'Mahony
Programme Assistant: Krystal Gaillard
Events Manager: Chris Irons
Editor: Anna Muizniece
Design: Elza Lőw
Rapporteur: Terry Brisco

Table of contents

Introduction

This report draws attention to the urgency to improve cooperation between the public and 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 second tabletop simulation exercise, 'Strengthening public-private cooperation in hybrid crises'. Following our 2019 tabletop simulation exercise, 'Hybrid warfare readiness: a tabletop exercise', Friends of Europe gathered once again senior officials and experts from NATO, the European Union, local and national authorities, the media and business 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 and the local level. Their involvement is essential as the private sector owns and operates a large percentage of the critical infrastructures being attacked and local authorities will be the first ones in line to have to deal with the consequences. The novelty of Friends of Europe's tabletop simulation exercise was to bring private sector representatives together with national and local authorities, as well as NATO and EU experts, to increase whole-of-society resilience.

The exercise was held under the Chatham House Rule to promote a free and open discussion. Participants were speaking in their personal capacities.

Executive summary

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

1. Involve the private sector in exercises and risk assessments at all levels to create resilience enterprise groups

There is a continued need for public-private exercises and risk assessments at the local, regional, national and international levels to build trust and the necessary connective tissue to enable more effective crisis response. This includes more involvement of the private sector in NATO's annual Crisis Management Exercise (CMX) and EU exercises, particularly within member states. Doing so forms local, regional and national whole-of-society resilience enterprise groups, which can also work together to anticipate future challenges and conduct joint risk assessments.

Subsequently, these same resilience enterprise groups can use the lessons from joint exercises and risk assessments to build local, regional and national whole-of-society response plans and recommend legislation.

2. Find the right balance between regulation and incentives

The right balance is critical to achieving effective public-private cooperation, especially before a crisis. There is a simultaneous need for more effective regulation of social media platforms and incentives to encourage key industries to share information and participate in information-sharing exercises.

3. Establish a public-private network of 'information first responders'

to detect and respond to disinformation early and prevent its further spread and traction within our societies.

As 'information first responders' need to have trust at local level, they don't need to be government professional communications experts but rather civic local leaders.

4. Conduct whole-of-society disinformation damage assessments

Both the EU and its member states, as well as regional and city leaders, should begin conducting whole-of-society disinformation damage assessments to inform decision-makers on where and how to shore up societal cohesion and keep disinformation from flooding the information space. This is especially vital since today's challenge is to simultaneously address a swayable general public that can be influenced by disinformation and the hardened and radicalised believers of disinformation.

5. Develop an EU Rapid Switch capability

The EU should explore the development of a Rapid Switch capability so that companies in key sectors could switch production to vital supplies, such as sanitisers, PPE and ventilators, in a crisis. Ideally, this would involve pre-arranged contracts to avoid corruption and cronyism.

6. Optimize the EU's physical and digital border management system with Frontex

Explore how the EU's physical and digital border management system with Frontex can be optimised to prevent conflicting national border measures during crisis situations, with a particular focus on organised criminal activity.

7. Establish an EU Rapid Response Network

with private sector critical infrastructure companies to provide rapid technical and recovery assistance to afflicted member states and partners. This should be based on a 'trusted supplier' network of EU certified companies.

8. Give Europol a mandate to assess and report annually on the link between organised crime and resilience within the EU

Context and aim of the exercise

When a crisis strikes, you want those who are responsible for managing it to be prepared, making sure there is continuity of essential infrastructure and services, preventing harm to communities, and having a plan for recovery.

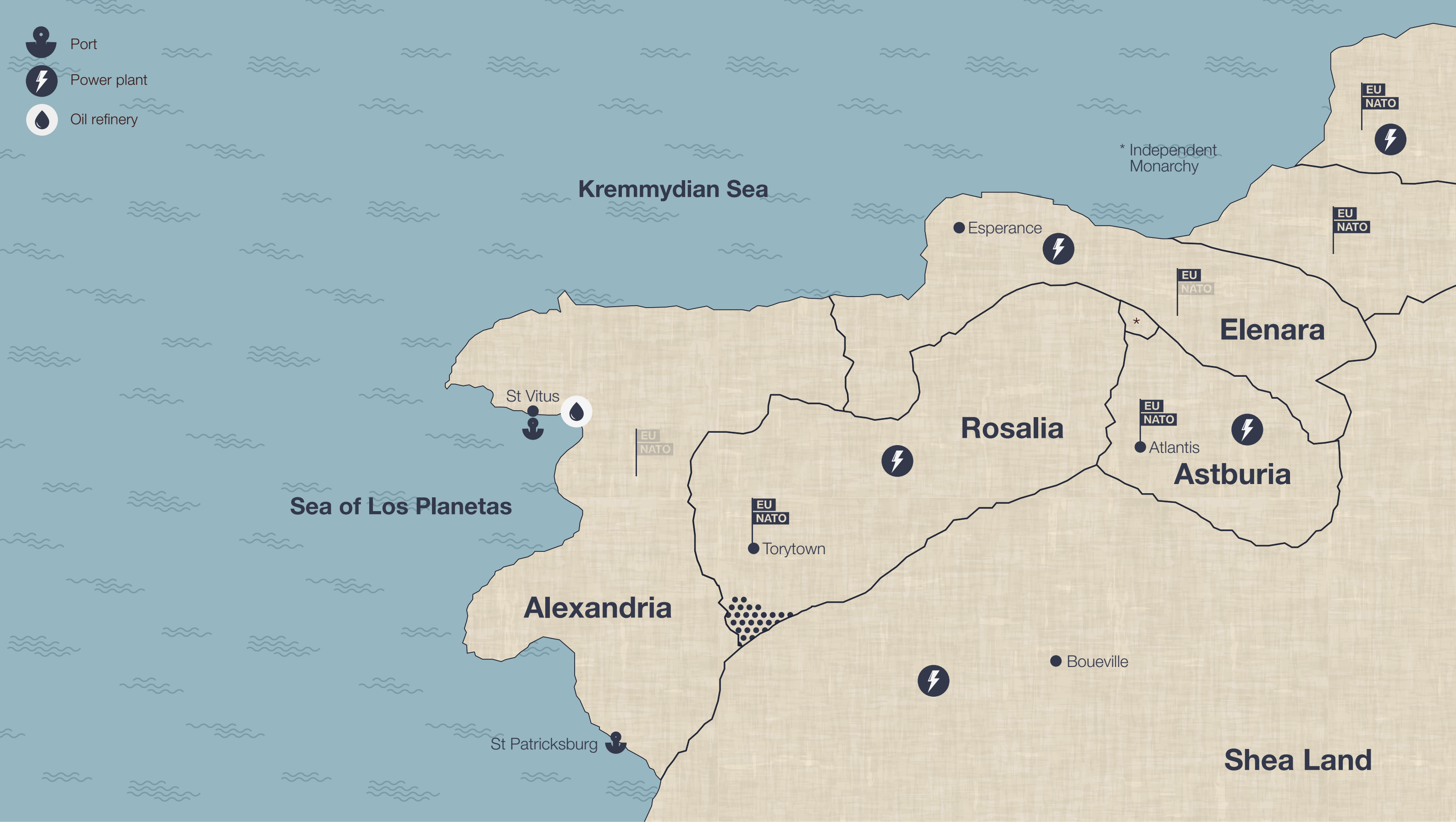
With 80-90% of all critical infrastructure owned and operated by the private sector in many Western countries, it is crucially important to ensure public-private cooperation is effective, communication channels are working and that roles and responsibilities are correctly assigned and properly understood when challenged by hybrid crises.

This is why Friends of Europe brought together 47 senior decision-makers and experts from the EU, NATO, national and local governments, the private sector and civil society to engage in a two-day online simulation exercise on a series of hostile hybrid campaigns.

The purpose of the exercise was to explore how governments, institutions and the private sector work together during a combined natural disaster and hybrid threat crisis and test the current state of public-private sector cooperation. Informed by the key takeaways of the exercise, we produced recommendations to improve cooperation among the key actors affected by hybrid crises in the future and increase the overall resilience of the transatlantic community.

During this exercise, we assessed whether we've plugged all the vulnerabilities identified in our 2019 exercise and what progress there has been, as well as how to deal with emerging issues like our increased reliance on resilient electrical systems and new developments regarding the impact of disinformation on societies during crisis.

For this second exercise, cities and local actors were also featured since they are the first line of defence and often serve as the first responders when we are faced with hybrid challenges.



Scenario

The exercise scenario was set in the fictional 'Fanuan Peninsula'. Five 'countries' in this region, a mix of EU and NATO members and non-members, were put under stress starting with a natural disaster leading to a major power outage and its cascading effects on various key systems - all during a new wave of the pandemic and amid the impacts of disinformation-driven violence we've experienced in the 2020-2021 timeframe. Other dynamics included increased short-term competition with each other over energy and vaccine supplies. As the crisis developed, it even led to escalating tensions with less friendly neighbouring states as a result.

"Our exercise is scenario-driven. We hope you will use it as a source of inspiration to develop your thoughts on the realistic situations described, under the banner of hybrid crises," said Jamie Shea, moderator of this exercise, Senior Fellow for Peace, Security and Defence at Friends of Europe and former Deputy Assistant Secretary General for emerging security challenges at NATO.

"We aimed for realism, so every incident in this scenario is something which has already happened in the past or is happening now somewhere in Europe," added Chris Kremidas-Courtney, exercise designer and Senior Fellow for Peace, Security and Defence at Friends of Europe.

Key themes explored in the 2019 exercise were further developed over the two days of this year's exercise. They included resilience of health systems and supply chains, often tested to breaking point in European countries by the COVID-19 pandemic over the last 18 months; climate change and its damaging impact on critical infrastructure; and disinformation and cybersecurity – all constant concerns for nations and businesses worldwide.

Conduct of the exercise: The Friends of Europe online simulation exercise brough together 47 senior decision-makers and experts from the EU, NATO, national and local governments, the private sector and civil society. Presented with a realistic fictional scenario, carefully crafted by the Friends of Europe team, participants were asked to deliberate on how to respond to a series of hostile hybrid campaigns. The scenario was divided into two linked rounds held over two consecutive days.

Participants received all the information about the scenario through dynamic videos and reading materials. Once this information was presented, they were divided into three breakout rooms: EU-NATO policy group, private companies and governments, and strategic communications and public affairs. Within these groups, participants discussed how to respond to the outlined threats and identify the way forward. Their findings and recommendations were then shared with the rest of the groups in a daily plenary session aimed at underlining the needs of each group and identifying potential structures for collaboration between them. In order to increase the dynamism of the conversation and make sure that every participant could contribute to the discussion, the plenary sessions were complemented by poll questions. The exercise concluded with a final session in which participants and facilitators shared their key findings and recommendations.

Main findings

"The time and resources invested in building public-private trust relationships pay for themselves fivefold when we are faced with a crisis situation. **You can't surge a relationship – or trust**," said Chris Kremidas-Courtney.

- The **first line of defence against hybrid threats lies outside of the government**. Not only is the private sector the first target of a hybrid campaign but our societies rely upon the **private sector** to restore basic services and provide unique capabilities to help governments gain situational awareness during crisis.

- Natural disasters and power outages **create opportunities for criminal and hybrid actors**, with criminal actors often being the first to take advantage of these situations.

- The need for **robust regional electrical energy networks is vital**. In a crisis, our neighbour's energy infrastructure weakness can quickly become our own.

- **Situational awareness (SA)** can be an even bigger challenge when there is no electricity to power the systems we rely on for SA. Local actors are more able to gain SA on the ground during power cuts, while national and international levels have unique capabilities which can assist local responders. Thus, being able to bridge these two entities during power outages is vital.

- Banks, tech companies and other **industries also have a vested interest in the stability of the economic and social system** and have unique capabilities which the government can tap into, provided they have a trusted public-private partnership.

- We must recognise and appreciate the **differing levels of public trust** in local and national governments, the private sector and civil society organisations and learn how to work together in a way to maximise public buy-in of crisis solutions.

- The **EU and NATO can start to take certain response actions** prior to a member state asking for assistance. Both should include key **private sector actors in EU and NATO resilience exercises** and planning processes.

- **Early diplomatic efforts** during crisis can create opportunities to improve relations by addressing the **urgent requirements of afflicted countries**, even if diplomacy must be conducted discreetly in order to be feasible.

- **A relationship with a regulator is not the same as a relationship with a partner**. Governments gain more trust with industry through incentive structures than they do by compelling companies to share information. That said, the business models of social media companies and the unique vulnerabilities they can create may require more effective regulation of their activities.

- Decades of lessons learned in countering and preventing radicalisation of violent extremists must to be applied to the recent phenomenon of **disinformation-driven violent extremism**. The EU's Radicalisation Awareness Network (RAN) is a key resource to address this phenomenon.

- The **importance of reaching marginalised groups** in times of crisis must be considered as part of a broader public communications plan.

- Renewed awareness that **immediate decisions** made to solve short-term problems during a crisis **can often lead to long-term problems**, especially in terms of which industries and populations are favoured.

Additional themes and findings

When communication breaks down

Effective communication during a crisis requires situational awareness, as well as excellent coordination. Reaching marginalised or isolated communities can be more challenging. Suggested solutions include more communication coordination with the EU and NATO, harnessing ethnic languages and/or NGOs to contact these target audiences, developing a social resilience strategy and calling on simpler channels such as radio.

Trust is also vital for communication, though it's increasingly in short supply. According to a recent Edelman Trust Barometer, we live in an era of low trust in governments: just 53% of respondents said they trust them, four points behind NGOs (57%) and eight points behind the private sector (61%). People often trust local authorities more in a crisis, especially when national governments are seen to be misleading their citizens. Thus, local-level communication strategies should be favoured wherever possible. It was also noted that trust is easily lost, hence the importance of governments getting their messaging right.

Multi-channel communication challenges

In an emergency, telecommunications companies are well used to shifting traffic between landlines and mobile connections, as necessary. They also have expertise in secure (encrypted) channels, which can help when fighting disinformation or insider attacks.

A telecoms expert noted that recent attacks on 5G towers had only a limited effect on mobile communication capacity, but this could change if the volume and speed of attacks increased. Operators may also fall back on 4G technology and will do so for the next decade. Even though the COVID-19 pandemic led to a 40% jump in mobile phone calls, the sector had plenty of spare capacity, underlining how the private sector can usefully play its part in a crisis.

Likewise, mobile operators are well used to threat intelligence sharing, often cross-border. However, during the debate, it became clear that private companies find it easier to cooperate with their counterparts or national authorities, while doing the same abroad is less easy.

Operational resilience

The EU and NATO are accustomed to cooperating on a regular basis. However, their crisis response mechanisms are not identical, which can lead to parallel requests for assistance being made by member states. This of course can be resolved through constant coordination and information between DG ECHO, the Emergency Response Coordination Centre (ERCC) and the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) as was witnessed during the coronavirus pandemic. Another positive development is NATO's continued emphasis on building its member state resilience as manifested in the June 2021 NATO Summit Communique, encouraging countries to build their resilience and further developing advice and guidelines on how to prepare for emergency situations.

Fighting false information

Disinformation is a growing problem for both the public and private sectors. Companies could play a greater role by removing false content online or amplifying information from trusted sources. The private sector does understand this problem and often closely cooperates with government, while raising awareness and offering training on it.

Disinformation is widely recognised as a key 'hybrid threat', since it disrupts decision-making and undermines trust within societies by creating an alternate reality. It becomes even more problematic when it targets key profiles such as politicians, journalists or online influencers. One of the best solutions to disinformation is to prevent it from becoming widespread, such as through public debate and awareness-raising with local actors proven to be the most effective in delivering these messages.

Extremism and radicalisation are increasingly driven by disinformation. For instance, anti-vaxxers have burned down vaccination centres in Italy and the Netherlands, while over 200 5G towers across Europe have been attacked by conspiracy theorists. Companies have been largely absent in efforts to prevent such attacks. Yet the private sector could become a 'key brick in a broader strategy' to target disinformation and extremism, especially if companies realised how their profits can be impacted by these issues.

Meanwhile, there is a worrying convergence of classical extremism, hate speech and disinformation. This situation could worsen over the next decade, as new technologies like AI-enabled bots, virtual and augmented reality and the Internet of Things become more common.

Prioritising energy

Any crisis – from food to health or disinformation – can be made worse when energy networks are down. Governments should therefore focus on energy resilience by establishing better energy connections between regions and countries. When we work with our neighbours to build a networked energy infrastructure, we help ourselves.

Energy crises, like any other crisis, can be staved off through better anticipation. Some companies already do this through their own security or business intelligence groups.

One key theme which emerged during the exercise debate was the need for public-private risk assessments to improve overall crisis anticipation and planning. Likewise, conducting similar cross-border public-private risk assessments and exercises can build cross-border relationships before a crisis hits.

Conclusion: preparing for the future by looking at the recent past

“Today, we’re shifting our focus beyond management of a crisis. We want to spotlight the cooperative relationships and mechanisms we need to help us better tackle problems like those in our scenario,” stated Chris Kremidas-Courtney.

On the closing day of the simulation exercise, the participants were posed general questions: if you could go back in time some 18 months, what would you change to prevent this crisis or make it easier to manage? What cooperative relationships do you wish you had spent more time building? What barriers to cooperation do you wish you had spent more time breaking down?

The responses were both informative and encouraging. Here are some insights and comments from participants:

- “If we could go back in time to change something it would be to regulate social media platforms and browsers, such as Google Chrome. Make sure that algorithms do not increase polarisation, make authoritative information easier to be found. Also, to make it harder for people to self-radicalise. Regulate big tech so they do not increase polarisation,” said one civil society representative.

- “12 to 18 months ago, we should have built better relationships and invested in staff because equipment, etc can quickly be built. Building better relationships would allow access to spare capacity either by having patients being moved across borders or having additional staff supporting foreign healthcare systems,” commented a health expert.

- “We needed to recognise that the energy resilience and autonomy of EU and NATO members is completely strategic. It’s necessary to anticipate such a crisis and to help each country develop energy distribution better both internally and across borders and regions,” a private sector representative noted.

- “18 months ago, we should have coordinated around sequencing earlier on (to identify variants), but also working better with hospitals. Public health institutions need to coordinate proactively to have a better appreciation of what the situation is and to compare and contrast at the local level and between countries.

- “We would have been honest about the precautionary principle: ‘we don’t know what we’re doing but let’s take precautions anyways’ (i.e. wearing masks much earlier on during the pandemic). 18 months ago, we should have adapted to the virage technologique in schools, etc and been ready for situations like this,” commented a health expert.

- "In hindsight – knowledge about disinformation is a key feature – public, governments, private sector do not have enough knowledge about disinformation practices. We should have identified activities online earlier and talked about what to do about them much earlier," a private sector representative noted.

- "First we need to see what intelligence we have about the attacks in all countries and see if we can coordinate or fill the gaps in national intelligence and ascertain if it is criminal activity, etc. This would be depending on the nature of the legal agreements with the countries to have access and share data. So, 18 months in advance, it would have been useful to have those agreements in place," said an EU representative.

- "We needed better regulation of social media platforms which, of course, would have to go much further back in time. Better tracking and adjusting of radicalisation. Creating networks of 'information first responders', trusted at the local level, that can be sharing reliable information," noted a communications expert.

- "I would push for regional energy connection, or in other words don't be Texas. No country or state can be isolated and Texas, is a perfectly good example of that. Power is key, without it, food becomes a problem, public health becomes a problem, information becomes a problem. So I think the key to everything at this point in our modern society, since none of us are self-sufficient is to ensure that to the greatest extent possible, we can keep our systems supplied with power.

- "What cooperative relationship would I have spent more time building? Assuming I was responsible for some aspect of public security, I would want to build a relationship with as many of my colleagues as possible across national borders. I would want the biggest virtual rolodex I could compile so that, if I needed help, I wouldn't have to introduce myself because, as many people have said- this over and over again, you can't surge relationships, you can't build trust in the middle of an emergency.

- "And finally, which barriers do I wish I had spent more time breaking down? What I would done in this scenario is look for the hardest problem out there and just try to find a workaround instead of just sitting on my hands," shared a national government representative.

- "I would stress the importance of recognising disinformation as a hybrid threat and that it needs to be dealt with coherently. We have quite good cooperation with state authorities, but I would have liked to see even better and closer, more awareness raising among them, together with us and the broader public," commented a private sector representative.

- "We should have held a joint TTX between government, policy and local service providers and used that to work together to establish a joint plan of action," stated a local authority representative.

- “The importance of understanding the drivers of behavioural change – what we’ve understood is that people needed to change behaviour very quickly and accept restrictions, and one of the things we needed to have earlier was messaging around health. [We] should have involved extra expertise, for example retail experts [and] transport experts. Shifting the patterns of people and how to keep people as separate as possible required expertise on how to get this messaging across,” noted a health expert.

- “If governments address no other aspect of cybersecurity, they must protect critical infrastructure. Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Every country is unique and there are no clear international rules about what should be vital in each and every country,” one cybersecurity expert stated.

- “People trust local initiatives and local authorities tend to be better suited to respond directly. What [to] do differently? Have localised networks in place before crisis. Akin to police and fire departments, have ‘information first responders’ in place,” suggested a media representative.

List of participants

Philipp Amann

Head of the Expertise and Stakeholder Management at Europol’s European Cybercrime Centre (EC3)

Lukas Andriukaitis

Associate Director at the Atlantic Council Digital Forensic Research Lab

Ruben Arcos

Lecturer and Researcher at Universidad Rey Juan Carlos

Cristina Arribas

Intelligence Analyst

Luís Barreira de Sousa

Ambassador for Cyber Diplomacy at the Portuguese Ministry of Foreign Affairs

Philippe Brezellec

Deputy Chief Security and Business Intelligence Officer at Engie

Hanneke Brouwer

Seconded National Expert at the European Centre of Excellence for Civilian Crisis Management

Laurence Clarkin

Vice President for EMEA Crisis Management at Citigroup

Gilles de Kerchove

Counter-Terrorism Coordinator at the General Secretariat of the Council of the European Union

Kostas Dervenis

Senior Sales Manager at Intrasoft International

Maria do Rosario Penedos

Counter-Terrorism Working Party (COTER) Delegate and Chair of the Horizonal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) at the Permanent Representation of Portugal to the EU

Amy-Anne Fairhurst

Global Head of Crisis Management & EMEA Head of Cyber Investigations, Citi Security & Investigative Services at Citigroup

Jon France

Head of Industry Security at GSMA

Jessica Giandomenico

Head of Research and Analysis at Earhart Business Protection Agency

Caroline Groene

Policy Advisor on Cybersecurity & Digital Diplomacy and European Government Affairs at Microsoft

Klaus Gundolf

Head of the Internal Crisis Management Team at Siemens

Jonathan Toby Harris

Member of the House of Lords, Chair of the National Preparedness Commission, former chair of the Metropolitan Police Authority and former reviewer of London’s terrorist preparedness

Vadim Ivanov

Deputy Director at the Estonian Rescue College

Ana Cristina Jorge

Director of Operational Response Division at the European Border and Coast Guard Agency (Frontex)

Andrej Kavar

PMG Coordinator at the Permanent Representation of Slovenia to the EU

Athanasios Kosmopoulos

Data Protection Officer at the Greek Ministry of Digital Governance

Stefan Kowitz

Director at the Multinational Medical Coordination Centre/European Medical Command (MMCC/EMC)

Adrian Lazaroaia

Senior Analyst of the Risk Analysis Unit of Situational Awareness and Monitoring Division at Frontex

Rosamund Lewis

Head of the Smallpox Secretariat, Emerging Diseases and Zoonoses Unit, Health Emergencies Programme at the World Health Organization

Hanna Linderstål

CEO of Earhart Business Protection Agency

Iivi Luuk

Policy Officer for Civil Protection Policy at the European Commission Directorate-General for Civil Protection and Humanitarian Aid Operations (DG ECHO)

Merle Maigre

Senior Expert on Cyber Security at the e-Governance Academy Foundation

Rémi Mayet

Deputy Head of Unit for energy security and safety at the European Commission Directorate-General for Energy

Tarik Meziani

Head of Unit for Media Operations at the Council of the European Commission Directorate-General for Communication and Information

Megan Minnion

Policy Officer at the North Atlantic Treaty Organization (NATO) Operations Division (OPS)

Juerguen Muntenaar

Deputy Director for NATO Matters at the Multinational Medical Coordination Centre/European Medical Command (MMCC/EMC)

Pauline Neville-Jones

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

Julian Patzina

Senior Security Manager at Siemens

Wayne Raabe

Director of Interagency Partnering at the United States European Command (USEUCOM)

Vira Ratsiborynska

Research Analyst at North Atlantic Treaty Organization (NATO) Strategic Communications Centre of Excellence

Clare Roberts

Senior Policy Coordinator for Hybrid Warfare/Resilience at the North Atlantic Treaty Organization (NATO) Operations Division (OPS)

Shaun Romeril

Lead Consultant at 2creatEffects, former police officer at the Metropolitan Police and former senior advisor for counter terrorism strategy

Tamsin Rose

Senior Fellow for Health at Friends of Europe

Alessio Rugo

Head of the Audit and Security Section at the Telematics Department - IT Service, General Command of the Guardia di Finanza

Shiho Rybski

Director of Exercises at The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

Burcu San

Director of Operations at the North Atlantic Treaty Organization (NATO) Operations Division (OPS)

Hans Schoemaker

Political Administrator at the Council of the European Union Directorate for Foreign Affairs, Enlargement and Civil Protection

Edvardas Šileris

Head of the European Cybercrime Centre at Europol

Sabrina Spieleder

Policy Officer at the European External Action Service (EEAS) Division Strategic Communications and Information Analysis

Alice Stollmeyer

Founder and Executive Director of Defend Democracy

Paul Taylor

Senior Fellow for Peace, Security and Defence at Friends of Europe and Contributing Editor at POLITICO

Renata Vertovsek

Head of Section for civil capabilities and crisis response at the Slovenian Ministry of Defence

Annex

Participants were divided into three breakout rooms to discuss the scenario: EU-NATO policy group, private companies and governments, and strategic communications and public affairs. These were their key takeaways:

Private companies and governments (facilitator: Chris Kremidas-Courtney)

- The primary public-private relationship is between the member state and the companies licensed to operate on its territory - not directly with NATO or the EU.

- Food and power services are vital as a first response to a natural disaster. It is essential to restore these basic services while remaining mindful that immediate decisions on food and water must be taken with care, otherwise this could lead to longer-term societal divisions.

- Governments' first reflex in public-private interactions is to coerce and regulate instead of first seeking dialogue and partnership. A relationship with a regulator is not the same as a relationship with a partner. Governments gain more trust with industry in incentive structures than they do by compelling companies to share information.

- That said, despite government's best efforts to seek dialogue and partnerships with social media companies, the unique vulnerabilities they can create may require more effective regulation of their activities.

- Situational awareness is especially difficult to achieve at local, national and international levels when electricity grids are down or unreliable. The public and private sectors can work together to develop alternative means which are essential to being prepared for such a crisis.

- It is essential to communicate with the public in order to prevent civil unrest and provide reassurance that the situation is under control. Analog methods, such as proximity policing and human contact by local actors, are essential when modern communication channels like mobile phones are unavailable.

- Natural disasters provide an opportunity for hybrid and criminal actors to take advantage of the situation, but criminal actors are usually the first to take advantage.

- Conduct more public-private exercise-s to prepare for hybrid threats but understand that it is necessary to create an incentive structure to attract private sector entities to participate. This could take the form of priority for government contracts, certifications which could lead to lower insurance premiums, or certain tax breaks from various levels of government.

- Energy network development: we must continue to develop regional energy networks because our neighbour's vulnerability can quickly become our own during a crisis.

- Public sector officials need to know how and where to find the private sector's plentiful expertise, such as behavioural specialists, in order to help government during a crisis.

EU-NATO policy group (facilitator: Jamie Shea)

- International organisations like the EU and NATO first need to receive a request from member states before they can assist, but they can and should still engage in contingency planning.

- NATO and the EU are both well-prepared for crises and have a good track record of responding quickly through the EU's ERCC, DG ECHO's EU Civil Protection Mechanism and NATO's EADRCC.

- European cities in crisis cannot directly seek help from the EU or NATO, as requests must go through national governments.

- Better intelligence before and during crises: both the EU and NATO are developing this, for example, through Copernicus satellites and the Joint Intelligence Security Division, respectively.

- The EU and NATO can quickly talk to one another in times of crisis, but there are potential issues over duplication of response efforts, pointing to the importance of focusing resources in areas of scarcity.

- Frontex, the EU's border and coast guard agency, can intervene if a humanitarian crisis arises; in this regional scenario, that could require law enforcement.

- Nations must define their own needs in a crisis before seeking international help and can project these needs best through periodic whole-of-society exercises which involve the private sector an civil society.

- Diplomacy, a soft power, can play a major role if used smartly and imaginatively.

- Situational awareness and intelligence are key in any crisis.

- An international crisis gives the EU and NATO a mandate to act and plan. However, if they are to cooperate better, their agendas should include similar topics (e.g. pandemics).

- When and how should the precautionary principle be invoked?

Strategic communications and public affairs (facilitator: Angela Pauly)

- Situational awareness: know who to address and how to set priorities for communication; the first step is to address basic needs, figuring out what they are and telling citizens what help they will get.

- Readiness to adopt simpler, more basic channels when modern ones are down, such as use of loudspeakers on vehicles, meeting people in the streets or going door-to-door.

- Understand what communications channels are still available and who controls them.

- Does the public trust the communication coming from certain authorities?
- When communication is re-established, ensure that social media platforms are available.
- Be ready to tackle harmful disinformation; monitor and map extremist narratives to inform efforts to prevent and tackle the polarisation of society.
- Create networks of ‘information first responders’ to detect and respond to disinformation early.
- Build forecast scenarios and planning responses.
- Establish communication partnerships with:

  1) civil society to build open groups on social media to challenge closed groups;
  2) NGOs to reach out to marginalised and isolated groups;
  3) local media; and
  4) local authorities to build trust, but keep open channels between local and national authorities.

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.