



Hybrid Threats

Summary Report


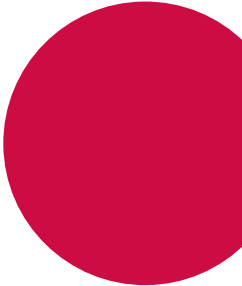
*National Security Council conference
on hybrid threats held at the
University of Iceland February 2020*



Hybrid Threats

Summary Report

*National Security Council conference on
hybrid threats held at the University of Iceland
February 2020*



Content

Opening Remarks

Katrín Jakobsdóttir, Prime Minister of Iceland and Chairman of the National Security Council 7

Keynote Address:

Security and Hybrid Threats

James Dipple-Johnstone, Deputy Commissioner Operations, UK Information Commissioner's Office ... 9

First Panel Session:

Conventional and Unconventional Responses to Hybrid Challenges

Antonio Missiroli, Assistant Secretary General for Emerging Security Challenges, NATO 17

Nora Biteniece, Software Engineer, NATO StratCom Centre of Excellence in Riga 20

Discussions 23

Second Panel Session:

Hybrid Defence, Safeguarding Democratic Values

Jurgen Klemm, Strategic Communication Advisor, Estonian Government Office 27

Discussions 30

Third Panel Session:

Importance of Fostering Resilience

Flemming Spildsboel Hansen, Senior Researcher, International Security, Danish Institute of International Studies 33

Kristi Narinen, Director of International Relations, European Centre of Excellence for Countering Hybrid Threats 39

Closing Remarks

Silja Dögg Gunnarsdóttir, President of the Nordic Council 41



Opening Remarks

Katrín Jakobsdóttir,

Prime Minister of Iceland and Chairman of the National Security Council

Dear guests,

It is a pleasure to open this conference on national security and hybrid threats. Democracy and human rights are constantly being challenged around the globe, through a range of coordinated methods, specifically aimed at confusing and destabilizing societies as well as undermining trust and democratic processes. Apart from blurring the lines between war and peace, these methods can include election interference, cyber-attacks, exploiting weaknesses in critical infrastructures, and economic and trade related pressures.

While disinformation campaigns and fake news are well known throughout history, the dissemination methods are more sophisticated than before. Algorithms enable micro- and macro targeting, create new possibilities to directly influence public opinion, or opinion and behaviour within certain groups. This may be performed by states or non-state actors, operating within or across borders, exposing the vulnerabilities to exploitation and abuse by those who have the resources to make these new technologies work to their advantages. Given the speed of new technologies the impact can be both massive and sudden.

In response, governments must be prepared to adopt laws ranging from screening of foreign investments to cyber sanction regimes to address what can be called grey zone risks. It is also essential to develop capacity to detect and understand malicious activities at an early stage and raise public awareness of the problem. At the same time we also need to deconstruct concepts, such as hybrid threats and warfare, and not treat them as novelties. Already in the mid 2000s, such concepts were a part of security and military doctrines and we can even go back to the father of containment during the early Cold War, George Kennan, who wrote in 1948 about the constraints of the idea of a clear difference between peace and war. In short, military power and forces have always been aware of the ambiguity between military conflicts and political warfare. Information can and has been weaponized as a part of an ideological struggle. Now it is often used in a normalized language to undermine social trust. To be sure, the mixing of non-violent subversive political acts on the one hand and violence and warfare on the other, has broadened the spectrum of threat perceptions. However, if too many factors are included in the definition of hybrid threats, it risks conceptual fuzziness.

Finally, we should also be careful not to inflate threats or engage in demonization or alarmist measures as a part of mobilization for political purposes. Hybrid threats are not only external, they can also stem from internal societal divisions, even if they can be exploited by external forces. We should not forget that social tensions and economic inequalities can also work to undermine democratic governments. Weak public debates more focused on thrills than actual facts may contribute to the same.

In this conference, the focus is on the manifestations of hybrid risks with regards to defence and democratic values and how they can be countered. When addressing these issues it is critical that it is done in an inclusive way, bringing together government, civil society, institutions of higher learning and the media. We must also avoid any temptation to frame our response to this challenge by parroting the methods of the enemies of open societies. It must be firmly based on the respect for democracy and human rights and not include actions that undermine the fundamental values that need to be protected or accountability which is the essence of any democratic system. This is pertinent in today's discussions of fostering resilience, which will only be achieved through education and with access to reliable information.

I would like to thank all those institutions that have made this conference possible and to thank our international guests for taking the time to join us here for this conversation. What will be discussed here is highly topical and important, and indeed such an interchange of ideas is in itself one form of democratic commitments which needs to be shown in a time of deep political anxiety and worldwide authoritarian threats. This is what the National Security Council of Iceland, which I lead as the Prime Minister, is very much aware of, so it has been our aim to open the public discussion on threats, to secure the democratic pillars of society.

I wish you all a very good and productive conference. Thank you.

Keynote Address:



Security and Hybrid Threats

James Dipple-Johnstone,

Deputy Commissioner Operations, UK Information Commissioner's Office

Dear colleagues,

Thank you for the invitation to speak here today. I hope to share with you this afternoon some learnings from our work and insight as to how we started to address some of the issues associated with hybrid threats and cyber security in the UK. I would also like to say a little bit about how we see the role of the data protection authority developing and providing resilience in such threats. I would like to be clear in doing so, that I am not suggesting a finding of, or attribution to, a particular party or threat in the context of our investigation into the use of personal data in the democratic processes in the UK. Rather, what I want to do is share with you our view of the issues and challenges we identified in our investigation and in particular, the learning we have taken forward in the hope of being usefully informed in our discussions here today.

For those of you who aren't aware of the ICO, we are the UK's independent data protection regulator. The commissioner is an independent officer, appointed by Her Majesty for a fixed term, and the office has its own revenue stream from a fee levied on data controllers and provided for in statutes. We have a remit that spans of data protection, some protection of critical national infrastructure, cyber security enabling data breaches involving personal data, and our interest in these is across a broad range of the spectrum of confidentiality, accessibility and integrity of data, with the focus on cyber enabled data misuse. By this we mean the failure to secure, protect and respect the privacy of our citizens and the deliberate unauthorized accessing, theft and use of that personal data. We work in liaison with our colleagues in the National Cyber Security Centre and with the National Crime Agency. If that didn't keep us busy enough in these modern times, we also have the responsibilities for the access to public information which isn't too far removed from today's theme after all. We mustn't forget that one of the key opportunities to counter disinformation is to ease the access to reliable and accurate public information. We have and we take action on a civil regulatory basis and also as a criminal prosecutor. The commissioner is able to bring her own cases before our courts.

„We mustn't forget that one of the key opportunities to counter disinformation is to ease the access to reliable and accurate public information.“

We are mainly in the UK but with the increasing international data flows we are much more active internationally, recognizing the borderless nature of many of the threats we now face. In particular, given some of the big tech platforms we are involved in, we work closely with our colleagues in the United States and the EU, but also increasingly much further afield. We also hold the chair of the international grouping of data protection authorities, the Global Privacy Assembly, and we are looking to support that work through the secretariat. This international cooperation role is important to us and it is well exemplified in the focus of my comments today, concerning Cambridge Analytica.

We saw from the evidence we recovered from Cambridge Analytica that they were operating internationally. They were linked to American and US based researchers, developing tools in the US election context, for application of the United Kingdom and elsewhere in the world. We also gained a glimpse from the evidence we recovered of their attempt to use jurisdictional arguments to avoid their responsibilities. It is highly likely that as recently as two or three years ago, such a conference as today's would have been perfectly possible without consideration or involvement of the data protection authorities. There were few authorities, mainly in Europe, few of those had investigative arms or cyber capacities, even fewer had regulatory teeth. Cooperation internationally and between data protection authorities and other national law enforcements, election and cybersecurity functions, was rudimentary at best.

Over the past two years however, that landscape has changed dramatically. DPAs have been transformed in terms of their powers and capabilities. The public are much more aware of their rights and of some of the risks facing them: Privacy has gone mainstream. You don't have to take my word for it, you only have to see some of the recent advertising from some of the really big social media and technology platforms, ever seizing, increasingly appointing differentiation service, not a problem to overcome. Our citizens routinely expect their personal data to be safeguarded. Our own survey of UK residents shows that cyber-attacks and political misuse of personal data are two of the highest areas of concern for them, when it comes to their privacy. I will say more about that learning later. But I reflect here that one of the key items of learning for us, from this investigation, was a clear public expectation that there would be a regulator there, to keep this personal data safe.

Turning to the case itself, it is vital that in any democratic society that political parties and campaigners are able to communicate effectively with voters, and social media has an important role to play in that. But it is equally vital for the integrity of elections in democracies that all organizations involved in political campaigning handle and process personal data in a way that is in compliance with local data protection laws. Political parties have a crucial role to play in this. They are the largest customers in the ecosystem and the ecosystem evolves to meet their needs. The degree to which bad actors can operate and pose a threat is therefore linked to the environment that is allowed legitimately to operate by those who give it credibility. Hence, our focus in our work is on the established political parties and campaign groups.

In recent years, political campaigning has become increasingly sophisticated, as new technologies and communication tools develop rapidly. I would echo the comments that have already been made. Campaigners now use ever more innovative tech-

niques to attempt to understand potential voters and target them with effective political messaging. The commission's concern is that the trust and confidence in the integrity of our democratic processes risk being disrupted because the evidence suggested that voters didn't understand the invisible nature of these uses of their personal data. However unintended, this poses a risk of hidden manipulation that undermines these processes. This must change. People can only make truly informed choices about who to vote for if they are sure that their decisions have not been unfairly influenced.

The messaging technologies used by political campaigners may vary and change over time. I am sure that will be the case, but they all need to be working from the same rules and laws when it comes to data protection and direct marketing, regardless of the method or future technological developments. So how did we end up here? Following the referendum in 2016 on the UK's membership of the EU, stories began circulating in the media, attributing data misuse as a reason for the result. Some of this was self-congratulatory, other items related to data sharing and misuse that raised potential concerns about data sharing, privacy laws and election laws. The then new commissioner, Elizabeth Denham, issued an initial call for evidence to understand how data had been used. Following this review, she established a major investigation to better understand, in more detail, the use of personal data in a modern democratic process, and to look at the whole ecosystem.

The investigation looked at both sides of the referendum arguments, all major political parties as well as campaign groups, the social media platforms and also a range of suppliers of personal data. We took the whole ecosystem approach to heart. The investigation eventually grew to be the largest enquiry undertaken by the office and possibly one of the largest investigations by data privacy authorities anywhere in the world. At its site it involved 15 investigators, dozens of organizations of interests and around 100 of direct individuals involved. The inquiry spanned the United Kingdom, the United States, Canada but also around 30 different jurisdictions around the world. As we found out more and as there was wider public concern, our parliament also became concerned. The House of Commons selected a committee on digital media, culture and sports and included it in its work on disinformation and fake news. Some of the examples that gave rise to these concerns I will share a little bit later in this presentation.

So, what did we find from our investigation? We uncovered a really complex picture of data flows. At the core of it was an organization named Cambridge Analytica and the individuals it was working with, who had a low awareness and appreciation of privacy laws, yet access to vast analytical capacity, large data sets, and it has to be said, a good imagination on how to use it. Our investigation identified activities at the margins of the jurisdiction of several agencies in the UK. Each of which was aware of these issues of the periphery of its remit but was fully engaged with its own core remit and was working through how to understand this activity, and importantly, take action within the constraints of laws and rules that were often unchanged since the days of pen and paper. What we found about the ecosystem surprised us a little, not least what has already been touched upon by the prime minister about the

„But it is equally vital for the integrity of elections in democracies that all organizations involved in political campaigning handle and process personal data in a way that is in compliance with local data protection laws.“



speed and ingenuity of the data flows and uses, as well as the tactics of some of our adversaries to avoid effective regulation. I think few of us had imagined for example that data gathered from mothers in a maternity unit in exchange for some free baby products could be combined, subject to political analytics, and resold via political party and then passed on to campaigns to help inform micro targeting of those mothers in a sophisticated way.

Unpicking and explaining this was a key result of our work. We identified that all the political parties to which we had made inquiries collected individual's data in order to identify interest groups for targeting and microtargeting of political messages. This was done both on a geographical basis, particularly focused on marginal constituencies awards, and also on an individual basis to attempt to identify potential swing voters and target them with messages. We found that all three of the main political parties also had their own central data basis, which were frequently updated in line with the electoral register and which were accessed according to how the political

„We've been sharing through the Your data matters campaign, how citizens can keep their personal data safe.“

party was structured for constitutional and data registration purposes, either at the central level or on a constituency party basis. This data was then matched with other data obtained by the parties' own individuals, including data given directly by the individuals themselves, for example by canvassing on doorsteps, email or telephone contacts but also survey gators. Sometimes this was obtained by the party from third parties, for example the maternity data that I men-

tioned. This then generated an individual segment or category based on lifestyle type information, e.g. what newspaper the individual read, where they shopped, that kind of thing. It was used to make assumptions about their preferences and opinions. That data was then obtained from a number of sources, including some commercial data brokers or from people who were connected by the parties social media presence.

Our investigation found a number of issues with this ecosystem. As a result of which we issued fines to Facebook, some campaign groups and a data broker, but we also made referrals to agencies to follow our actions against some specific named individuals. We prosecuted Cambridge Analytica before the courts and secured a conviction and a fine and in the course of the investigation the company ceased trading. We also identified a significant set of recommendations for the university- and the political sectors. One of the issues of the file was that information that had been gathered by researchers, through the ethics process and with research at universities, had then found its way into the political system. We also collaborated with other regulators around the world to begin to contest the patterns of the behaviour that we saw, and there is still some final work ongoing to this very day.

What we have seen though is that some of the adverts that were originally out there, and these are on the select committee page, so you can see some comments on the European Union wanting to kill a cup of tea, that were then used to gather and recycle data and feed it into the process. We have then seen the evolution to ever more detail about how some of the parties are campaigning with an already identi-

fied presence. In the latest election much more detailed and clear messaging around who is paying for what advertisement and who is targeting what messages.

So, what learning did we draw from this investigation, as a data protection authority? First, that there were these data sets, these vast data sets, and access to them that proved to be just too easy. Some progress has been made since, but recent research done in the UK suggests that around half of all boards do not fully understand where and what their data assets value is, and security arrangements are, and this makes that data potentially quite vulnerable. We have also found that the dynamics between academic institutions, the private commercial sector, social media platforms and public activities is underpinned by these data flows and we exposed that through the course of our reports. We also found as a regulator we need to work better with others, so we engage with all these organizations,¹ in the course of our investigation and that capacity and capability for data protection authorities is crucial. We need to be able to flex our resources and meet the ecosystem demands and cover the broad waterfront of activity. So, for example within the ICO a part of the learning we have taken is to institute a standing team of our intelligence, investigative and audit staff to lead on this high priority work.

In subsequent elections in the UK, we have deployed these resources in real time, so we can follow up concerns, provide compliance advice to those involved in the process and flag threats during the election cycle, rather than waiting for the end. Another key part of the learning was the complexity of the technical challenge that cannot be underestimated. We adopted within the ICO, because of the background of a number of the staff, a police incident room-based approach with quite structured mechanisms of gathering data, analyzing it and then taking action. Even then, with an inquiry that generated 700 terabytes of data and evidence, that was quite a challenge to organize and to be able to make sense of. We also learned that the international dimension was vital, and part of the learning for us has been that it requires standing arrangements to be in place for cooperation with our counterparts, and that is behind our work with the Global Privacy Assembly. To make sure that the international instruments are in place to allow data protection authorities to work effectively together. We have learned the hard way that it's challenging to be building these relationships in the middle of an investigation, much better to have those relationships in place from the start.

What we have also learned is that the whole ecosystem approach is the right way forward. The previous very traditional model of investigations would have seen data protection authorities just looking very narrowly at the privacy issues and those established organizations within our regulatory radar. The challenges of the issues for example in the context of the referendum, of specific issue campaign groups that spring up, undertake their activity and then close down relatively quickly, were significant. There was a lot of activity and the potential for the evidential value that the activity to be lost was great. In the same vein, just the content of the messaging is of interest to us, the financing of the advertising and importantly the source and the method and the targeting of the message is also important. This is where, if I

¹ ICO, information commissioner's office; NCA, National Crime Agency; Cabinet Office; The Electoral Commission; National Cyber Security Center, a part of GCHQ and the Department for Digital, Culture, Media & Sport.

can cast to the future, where I think data protection authorities have a key role to play. We also need to embed this joint working, since then we have also undertaken incident response, tabletop and common threat analysis with our partners. We have regular meetings now and information sharing with our colleagues in the National Cyber Security Centre and the National Crime Agency. We combine the thematic insights from the data breach reports we receive under the GDPR, with their high level insights to make sure that we both understand that the high level threat picture as best we can so we can then build that into our proactive inspection and audit work as a data protection regulator. We strengthened our colleagues at the cabinet office teams to make sure that alongside the election commission we have a means to surge our resources in the critical election cycle, and importantly in the period right before the election cycle if necessary.

We have brought together these multidisciplinary teams of investigators, auditors, policy specialists, technologists and cyber teams to work together on these challenges. But resilience can't just come from the regulators, it has to come from the public as well, so we focused on public information and awareness. We've been sharing through the Your data matters campaign, how citizens can keep their personal data safe and we've continued our work to explain the ecosystems of data use, so that citizens can react accordingly. We have also looked at ourselves and how we can improve our laws and ways of working and agility. We have been keen to share the learning there. We know the law led to consideration for change in the UK and EU level, as well as further afield. The parliamentary select committee has also been influential in taking forward our recommendations with theirs to assist parliament in framing new arrangements and laws and will shortly be producing some political party guidance to help them handle data effectively.

This continues to be an area of work and a source for ongoing concern for data protection authorities. In our conference in Tirana, at the end of 2019, we agreed resolutions for further work on the use of personal data laws to tackle extremist content following the terrible events in Christchurch, but also as one of the policy themes to see how we can work better as a data protection community to build resilience in our own local communities. We've started work looking at the role of privacy rights in supporting democratic engagement, and for our part at the ICO, we have not forgotten the whole ecosystem approach, and we've been following up with the credit reference agencies and the data broking industry in the UK, to make sure these issues are addressed. Our findings have also fed into our own national guidance and we will follow up with the university sector around the use of research data and the ethical considerations involved with research projects with large amounts of personal data. With that we have been assisted on the inside by our colleagues at the Centre for Data, Ethics and Innovation, to make sure we are not stifling innovation, but actually supporting it down the right path. It's not privacy or innovation, its innovation with privacy.

In the UK there are continuing enquiries by the standing committee of the House of Lords, the Democracy and Digital Technologies Committee and they are looking at the continuities, challenges and future impact on democratic processes of new and emerging technologies. One area we are contributing to is our investigation to the Artech industry as well as continuing our work to monitor the ongoing election and

data uses. Of interest perhaps to the group is that lately the UK government has advanced work to improve the regulation on online harm content, including extremist content, disinformation and political messaging. We will work with the new regulator to ensure that the regulations in which way the messages are targeted, as well as the content, are regulated seamlessly.

I hope that this overview of our investigation, the issues it raised and the next steps has been helpful in encouraging some thoughts and considerations for your discussion this afternoon. This is a vital area for all our democracies. Technology has a great potential to invigorate our civil discourse and increase our civil engagement and that is all good. It will however need public confidence to do so and citizens will need to have insurance that privacy is being properly respected and data laws properly followed in that process. It will be a team effort across a range of players and data protection authorities, in my view, that will have a pivotal role to play and I am sure that there is a good will between us all to make this a success and I look forward to our discussions this afternoon.

Thank you.

„Technology has a great potential to invigorate our civil discourse and increase our civil engagement and that is all good. It will however need public confidence to do so and citizens will need to have insurance that privacy is being properly respected and data laws properly followed in that process.“

1.

First Panel Session:

Conventional and Unconventional Responses to Hybrid Challenges

Moderator:

Pia Hansson,

Director, Institute of International Affairs, University of Iceland



Antonio Missiroli,
Assistant Secretary General for Emerging Security Challenges, NATO

Ladies and Gentlemen, your Excellencies,

Good afternoon,

It is a great pleasure and honour for me to be here today. I had the privilege more than twenty years ago to meet Alyson Bailes, who taught at this university for a long time and I also had the privilege to stay in touch with her for many years. I have to say that she is still missed, and her acumen and lucidity in analysing emerging security challenges would be of great benefit to all of us today.

Let me start with a little anecdote. Right after the Cold War, when NATO had to adapt to an entirely new strategic environment, a NATO officer, a former colleague, compared the situation to “painting a moving train” or if you prefer “fixing a running car”. One can only sympathise with that appreciation. NATO did indeed change radically in terms of policy, strategy, military structure, outreach and even members. Today we are asked to paint yet another moving train, to fix yet another running car. Only this time our train moves even faster and is partially invisible, the car is partially inaudible. I’m speaking of course about the need for NATO to adapt to respond to hybrid threats.

Hybrid threats are indeed a unique challenge for an organization like NATO. They blur the lines between peace, crisis and war. They aim to undermine political cohesion by trying to amplify divisions amongst societies. They create ambiguity to complicate consensual decision making, and they can undermine NATO’s military responses in a crisis, for example by disrupting NATO’s reinforcement efforts. How must NATO adapt then, to meet the challenge of hybrid threats? What kind of strategies must we adapt? What specific tools must we build to deter or defend against hybrid aggression?

Step one, we must advance our situational awareness, we must be better at connecting the dots. Are for instance, a cyber-attack against a harbour here in Iceland and a simultaneous fake news campaign in Norway or Denmark just random events or are they a part of a planned hybrid campaign? One way to find out is to improve our intelligence sharing. A few years ago we established a joint intelligence and security division in NATO’s international staff, which includes a unit specifically devoted to analysing hybrid threats. The JISD has proven to be a successful bureaucratic innovation, providing us with solid analysis about hybrid actors and their methods.

Step two, we must continue to exercise challenging hybrid scenarios by introducing hybrid elements into exercises for our military and political decision makers, to address dilemmas that hybrid threats can pose. For instance on how to cope with

„Hybrid threats are indeed a unique challenge for an organization like NATO. They blur the lines between peace, crisis and war. They aim to undermine political cohesion by trying to amplify divisions amongst societies.“

the question of when to initiate collective action as NATO, in cases where an opponent's attack stays below what we call the kinetic level, the traditional military level, with tanks crossing borders or planes hitting military bases. If NATO were to wait with collective responses until an attacker deploys kinetic means, a dangerous gap could emerge between aggression and reaction. Inaction that could lead to escalation. Consequently, NATO needs to look much more closely into collective response options below the kinetic level. Last May we carried out a crisis management exercise called CMX19, in which cyber and hybrid elements, in the High North incidentally, were tested and exercised in a real type situation. Two days ago the North Atlantic Council had a scenario based discussion on that same scenario again and later this year the same kind of scenario based discussions will be carried out with our Finnish, Swedish and EU partners.

That brings me to the third step. The need to create specific tools, such as our counter hybrid support teams. A counter hybrid support team consists of civilian experts who could be deployed with an ally's request. An ally must demand the deployment of such a team, and these teams can be deployed in times of crises to show that NATO is vigilant and at the same time it demonstrates an act of solidarity with that ally. However, given their expertise in strategic communications, counterintelligence or the protection of critical infrastructure, such a team can also act as an advisory team to improve national structures to withstand hybrid threats. Counter hybrid support teams are a sign of NATO developing options below the threshold of Article 5. To be sure, allies have also stated that hybrid attacks can trigger Article 5, but our emphasis now must be on what our military calls "left of bank scenarios and situations".

Step four, deepening relations between NATO and the European Union. Our goal must be to bring our different toolboxes closer together. For example, through informal co-

„The need to create specific tools, such as our counter hybrid support teams. A counter hybrid support team consists of civilian experts who could be deployed with an ally's request.“

operation at the working level, both institutions have developed playbooks to coordinate their respective responses to hybrid activities. We have also started to engage in what we call parallel and coordinated exercises, and cooperation is facilitated by the European Centre of Excellence for Countering Hybrid Threats, recently established by Finland. I am sure that Kirsti Narinen will give you more information about their work and their plans, later this afternoon.

Step five, enhance national resilience. Since most hybrid attacks are within individual nations, NATO

must ensure that each member country is resilient enough to continue to perform as a reliable ally, for example, whenever NATO is planning to send reinforcement during a crisis. The 2016 Warsaw Summit Declaration highlighted resilience as the basis for credible deterrence and defence. In line with that statement, allies have pledged to improve their resilience to the full range of threats, including hybrid threats. The strengthening of resilience is a national responsibility, but NATO has produced guidelines that can serve nations as a benchmark for national assessments in areas such as energy or strategic communications. These requirements are regularly updated in the face of new developments, including the introduction of 5G communications standards.

Step six, attribution, in other words naming and shaming the hybrid aggressor. Strictly speaking attribution remains a sovereign decision by each state. However, we recall when a Russian agency attempted to kill a former double agent in the British city of Salisbury in March 2018, most NATO and EU states publicly attributed the assault to Russia. Equally importantly, NATO allies and partner countries expelled numerous Russian diplomats. Such actions could have a deterrence effect on at least some actors. Even if collective attribution remains to be a politically delicate issue, we need to continue to persuade. You may have followed the case last week, of the public attribution that Georgia made on the cyber-attacks against the country's major media channels in late October in 2019, which was followed by statements from a number of NATO and EU countries worldwide. I would suggest that you compare the nature of these statements, some of them attributed to the GRU along the Georgian statement, others basically condemned the activity but didn't mention the actor behind, and there lies a nuance that has to be taken into account in different national approaches.

Step seven, new meetings formats. NATO traditionally meets at the level of foreign and defence ministers and occasionally heads of states. However, hybrid challenges go well beyond the remit of defence and foreign ministries. This is why we are bringing in additional actors. In May last year for example, we had the first ever informal meeting of the North Atlantic Council with national security advisors, and other senior officials dealing with hybrid threats. This meeting underlined the need for a whole of government approach in dealing with such threats and I would hope that it helped us slowly break down the institutional barriers that are still hampering our work.

Ladies and gentlemen, this brief overview of NATO's response to hybrid threats will hopefully have made one thing clear. NATO can paint a moving train, even if the train is a high speed one and even fix a formula one car along the way. The key to success is not to fall into the trap of mistaking hybrid for some kind of miracle style strategy against which there is no cure. Hybrid is not a miracle style strategy, if we keep improving our awareness and resilience and if we continue to deepen our relationship with the EU, we can demystify hybrid as a strategy that can be effectively detected, potentially deterred and eventually defeated.

Thank you very much.



Nora Biteniece,
Software Engineer, NATO StratCom Centre of Excellence in Riga

Good afternoon,

To set the scene for today's discussion, I would like to tell you about a case study we did a year ago. Before I start, NATO Strategic Communications Centre of Excellence is not a part of NATO's chain of command even though NATO is in the name. The aim of the centre is to enhance NATO's strategic communications capabilities through research, experiments, doctrine development, training and education.

The case study we did a year ago, during a national military exercise in Latvia, we practically assessed if we could gather enough public information about the participants and the exercise to influence their behaviours in the exercise, in a way that would act against their orders. Here is what we did. First of all, we set up a honeypot, something we would use to lure military service men and women to disclose that they were participating in this particular exercise. The second step was to expand our network of known exercise participants, the third and fourth steps were on the one hand to do research on the known participants, in order to find out as much information as possible about them, their weaknesses and vulnerabilities. Secondly, to monitor the exercise itself. The last step, but not least, was to reach out to these participants and engage with them. In this step we used social engineering techniques as well as other techniques to achieve our goals. In practice it looked more like this:

- Creation of false personas
- Honeypot pages on Facebook
- Closed group on Facebook
- Direct and indirect engagement through social media
- Creation of a merchandise selling website

Three weeks prior to the exercise we started creating fake profiles across different social media platforms, Facebook, Instagram, YouTube and Twitter. We created a fake Facebook page for the exercise which mimicked the official communication of the Latvian armed forces and we only posted legitimate information on that site. We marketed this page to a group we thought might be taking part in the exercise, that is people aged 18-55, living in Latvia, interested in or employed by the armed forces. Anyone who has done Facebook ads knows that it is easy to narrow down your audience to even such metrics as employed by or interested in the armed forces. We marketed this page to reach the possible target audience and once we gathered a significant number of followers, we created a closed group which we then used to lure participants in. The next step was to both directly and indirectly engage with the people we knew were taking part in the exercise.

Another step we took illustrates that not all attack factors are successful, this was the creation of a t-shirt and selling it on the website with the exercise merchandise. This didn't work out, but all other attack factors were successful. During the first week of our operation the Ministry of Defence and armed forces quite quickly noticed the fake page and reported it to Facebook, but nothing happened. They were unable to receive support, so they circulated a message around the armed forces, instructing people not to follow or share messages from the fake page. The second week we continued operating. We created the closed group, we received over ninety people as group members, and again we advertised to promote this closed group. In the second week, only after State Chancellery got involved, Facebook finally suspended the page. Which of course in a crisis scenario is unacceptable, that you have a fake page gathering information on your military personnel for two weeks before Facebook does anything.

Overall, the page operated for two weeks and gathered over 320 followers. It was suspended but the group was never suspended and is still active today. The overall results are that we identified a significant number of individual participants, we also identified exact locations of several battalions and troop movements timeframes for active phases. We also managed to induce certain behaviours. We used a range of social media platforms and dating apps and we actually got the GPS locations of reconnaissance units and we managed to get two people to leave their barracks while on exercise to meet a fictional girl.

Here are some examples of the things we noticed during our experiment. We messaged armed forces personnel from a fake profile asking which battalion they were from and when their active phase would be. This is just to illustrate that people do not apply the same security measures they do in the physical world to the digital world. This extends beyond the armed forces. It could just as well have been a fake profile promising financial gain in return for a particular behaviour. People just don't regard the digital environment as unsafe as the physical environment. In the closed group we also asked anyone who is a part of the 17th or the 19th battalion to come forward and in the comment section people actually replied. This group is unofficial, and this post is made by a fake profile and people answer.

„This is just to illustrate that people do not apply the same security measures they do in the physical world to the digital world.“

Another example we came across was on a dating app we used to identify and engage with the exercise participants. By using the app, we got information about their first name, last name, age, distance from our fake location and their unit. Because one individual posted a picture of himself in a uniform, military police, we could tell that his whole convoy was within five miles from us. We cross checked the information we gathered about this person from other social media platforms and online sources and found out his occupation, income and found out that he has a partner and a child but is still using a dating app, which indicates that this person is a good target, because he has something to hide.

What made it so easy and cheap for our small-scale operation to succeed? First of all it was Facebook's own targeting advertisement mechanism, we didn't have to do anything else but to say to Facebook that we wanted to reach anyone aged from this to that, in Latvia, interested in or employed by armed forces, and they did the hardest part of the work for us. Second, the "closed group" feature and "suggest friends" fea-

ture. Closed groups are quite popular on Facebook and other social networks such as Contacted. They allow actors to interact with people unchallenged because nobody who is not a part of the group can see what goes on. Here we actually noticed, as our experiment progressed, people started to become more resilient, if they posted comments saying which battalion they were from, after a few hours they would be deleted. The more we posted, the less answers we got. People got more resilient as the experiment proceeded, which suggests that there was some sort of self-organization within the target group that noticed something was going on, and they adapted quite quickly. The reach out and engage step was made quite easily because of the data we collected on the people. We were able to get their phone numbers by search engines, which is an unregulated business at the moment - if I am correct, dating apps and social networking sites.

The broader conclusions from this experiment are that the digital environment does hold enormous amounts of data on each individual and this data can be gathered legally, so we didn't do anything illegal. We broke terms of service on Facebook, Instagram and YouTube, but we didn't do anything illegal. Soldiers and security services are not the only targets for such attacks, social engineering and impersonation. Basically, any organization of importance is already a subject of these kinds of attacks. Education regarding these risks in the online environment needs to happen. We also

„ ... the digital environment does hold enormous amounts of data on each individual and this data can be gathered legally, so we didn't do anything illegal.“

believe that the best way to train your personnel or your public servants as well as the general public is to Red Team on them basically. First of all, during this experiment we found out the latest techniques, how to fake phone calls in Latvia and where to gather data from. We did our own research into the tools and capabilities available and trained our people. During this exercise we trained and tested the communications and reporting mechanism of the Ministry of Defence and the armed forces themselves, which was very useful as well.

Why is this even a thing? How does this fit into hybrid threats? There are different influence methods within different societal groups. Social media is largely used by younger generations so this is the vector that will be used to influence them. The aim of it is to affect without kinetic activity. So to influence someone's decision making.

Thank you.

Discussions

*Moderator: **Pia Hansson**, Director, Institute of International Affairs, University of Iceland*

*Panelists: **Antonio Missiroli**, Assistant Secretary General for Emerging Security Challenges, NATO, **Nora Biteniece**, Software Engineer, NATO StratCom Centre of Excellence in Riga, **Helga Þórisdóttir**, Data Protection Commissioner, the Icelandic Data Protection Authority, **Björn Bjarnason**, Rapporteur on Foreign and Security Policy on behalf of the Nordic Foreign Ministers, **Sveinn Helgason**, Strategic Communications Officer, NATO*

Four main themes emerged from the discussions following the speeches in session one. They are: 1) The fourth industrial revolution, 2) Social media, 3) The nature of hybrid threats, 4) The role and responsibility of authorities in regards to hybrid threats and cyber security.

This discussion summary is supposed to give an overview of the debate in the panel and not represent individual views and opinions of participants.

Fourth Industrial Revolution

Participants in this panel discussed the ongoing fourth industrial revolution where the big thing is data, including personally identifiable information. This is a concern regarding hybrid threats as personally identifiable data is being used by governments as well as both public- and private actors in all sectors, every day. That is really the big thing, how our data is being used.

Already the current technology and systems such as Google search engines, YouTube or Netflix recommendations, or in fact any system or digital media service that uses sorting algorithms, is making the users more exposed to tailored experiences. Nevertheless, most people are still turning a blind eye.

To minimize the threat this poses to our democracies, voters need to understand the digital environment they live in, how they are constantly being shaped by social media and search engines. Voters have to be

educated about these systems to be able to recognize things like deep fakes. Training and education have to be a part of technological developments and we as consumers should demand more transparency from these gigantic tech companies, using our information.

Social Media

Participants also used examples like the Cambridge Analytica case, which have demonstrated that people have been micro targeted without even realizing that they were being targeted at all. Social media offers political parties' direct access to each and every voter and by using the right technology they can micro target the voters there within.

Google and other search engines are also influencing us all the time and the search results one person sees is different from the results the next person gets. The more we use these search engines, YouTube, Netflix and other social media platforms, the more we get shaped by them. The lack of transparency and regulations around these platforms is a cause for worries.

In Iceland, 9 out of 10 adults use the same social media, namely Facebook, and 99% Icelanders use the internet each and every day. This makes it easy to follow and predict the discussions of a whole nation. It might be a small one, but we are still talking about a whole nation there.

The Nature of Hybrid Threats

Participants moreover highlighted that hybrid threats are a complex issue with no simple solutions. Hybrid campaigns are usually not limited to disinformation, they can include coercion, corruption, provocation, foreign accusation and jamming up communications, to name some examples. Hybrid campaigns, as we know them, tend to be tailored to specific situations and the vulnerabilities of each target, even if they use similar methods and follow recognizable patterns.

In the cases of electoral campaigns, hybrid campaigns focus on the issues that could be used to divide the society even further and thereby make the position of the future government more difficult than it would have to be. They search for economic weaknesses to exploit, such as foreign direct investments, specific interests in the region, natural resources and so on. Issues they see fit to use as entry points for sophisticated campaigns.

Finally, a point was made that we should not look at hybrid campaigns as threats as we are constantly under attack already.

The Role and Responsibility of Authorities with Regards to Hybrid Threats and Cyber Security

Finally, the participants in this session discussed the power of those who have the know-how, will and opportunity to target people on social media in order to influence their behaviour, e.g. how the targeted person votes in elections. The linkage between this power of influence, threats to national security and the importance of data protection should not be underestimated.

The devices people use in their everyday lives are increasingly becoming connected to the internet and

thereby increasing the risk that anyone can gain access to personal, identifiable information. Questions were raised about the security of our critical infrastructure, considering hybrid threats, e.g. when medical devices in hospitals are connected to the internet and personal medical records are kept online.

How far can governments go in countering these threats, in the name of national interests and security? There are responsibilities and limitations, the constitution e.g. states that privacy must be safeguarded. In the case of Iceland, it is interesting to think about what means the government has. There is no military and the defences are based on civilian means. NATO offers guidelines, but nonetheless it is a national responsibility to counter hybrid threats. Iceland has a data protection system, based on civilians to defend the market and make sure that our personal data is protected, but this is a much broader issue.

Iceland is a very digitalized society but doesn't have the necessary defences in the case of hybrid threats. That is a very serious issue. The country is on top of the list of the use of internet, broadband and so forth, but when it comes to internet security Iceland is low on the list. This is an issue with regards to national security and something that Icelandic authorities must look into.

The way forward for those defending against hybrid threats, whether it is the government, public or private actors, is to exercise and map possible scenarios. Who are the possible aggressors? What are the potential campaigns? What are our weaknesses and possible targets? What is their strategic aim? How could we respond? Even if this needs to be incorporated into our national security structure there are limits to what the government can do, and the issue calls for wide cooperation between different actors and agencies.

There are several reasons for the limitations of government actions countering hybrid threats:

a) Most cyber incidents and hybrid campaigns (about 70%) stem from individual's own endeavours, the individual's own sloppy behaviour online. This calls for enhanced education on cyber hygiene. Often the consumer in us goes against the interests of the citizen in us, and this is something that everyone needs to be aware of, but there are limits to what states can respond to.

b) Most of the social media platforms and communications networks are privately owned and privately operated. States do not control the internet and states do not control social media. This is a very important point to keep in mind and therefore the degree of cooperation with the private sector, in creating an environment where this is possible, is essential.

c) Western countries don't want to restrict the freedom of their citizens, through the ownership of social media platforms, or by limiting freedom of expression.

It is important to keep in mind that these limits exist and that this is a long-term issue demanding cooperation between individuals, society and governments.

2.

Second Panel Session:

Hybrid Defence, Safeguarding Democratic Values

Moderator:

Sveinn H. Guðmarsson,
Press Officer for the Ministry for Foreign Affairs

Jurgen Klemm,
Strategic Communication Advisor, Estonian Government Office



Firstly, I would like to give you a brief overview of the Estonian Government Office stratcom team. What it is that we do. After that I will give you an example of a Russian information campaign that we faced lately, and to some extent are still facing and at the very end I will draw conclusions and discuss the possible lessons to be learned.

I have to begin with going back to the definitions. In my presentation I use encyclopaedia definitions that means you can Google and within five minutes you should get the same result or the same explanation. The encyclopaedia definition or the Googling definition of hybrid threats is that there are four steps that the actor needs to do or go through.

Firstly, when we talk about hybrid threats, we talk about the actors trying to undermine trust in society or in the democratic institutions. For example, in elections or the judicial system or the freedom of the press. Secondly, we can talk about hybrid threats when somebody is putting our social values up for question. Do we need freedom of the press? Do we not discriminate, or do we even respect the rule of law? It is our values that are being questioned. Thirdly, they try to gain political or geopolitical influence. This can range from having very specific aims, like trying to influence the implementation of financial sanctions, or it may be much less specific, like influencing elections or trying to convey the image of doing so. Fourthly, they try to affect decision making, whether it is on the individual level, the societal level or the political level. What hybrid aggressors aim for is: undermining trust in democratic institutions, questioning societal values, gaining political influence and affecting decision making.

This is where the Government Office stratcom comes in. Firstly, we raise situational awareness. Hybrid campaigns, to some extent, always include the public sphere through the distribution of public information through the media. Therefore, we have to be aware of what is going on in the media. We have the capacity to monitor the media around the clock, that is both the Estonian and Russian speaking media in Estonia, as well as the whole information apparatus of the Russian Federation. This also means monitoring media spheres in western countries we take interest in. We need to closely follow discussions about us, to be able to detect if the discussion is being manipulated. Since we have been talking about values, we need to survey public opinion - polling; and this is something every government does. We aim to put more effort into such surveying, in order to get a broader picture of polling across the government. This is necessary to, firstly, find the weaknesses in the values, and secondly, to be able to compare between years if there have been any changes in the values.

„What hybrid aggressors aim for is: undermining trust in democratic institutions, questioning societal values, gaining political influence and affecting decision making.“

Secondly, we try to build resilience. Detecting fake news and increasing media literacy are examples of such specific assignments for us. We have to figure out ways to work towards higher media literacy.

Thirdly, narratives of history. When somebody claims that it was actually Poland who is to blame for the Second World War, we have to stop and think about it. How do we help the historic narratives that the actor is trying to push? How do we do the counterpart?

Fourthly, in every situation our message, from the state, has to get across. That is crisis preparedness. It is how the government communications work in a crisis situation.

Now to the Russian information campaign. For this I have to take you back to the year 2014, when Russia annexed the eastern part of Ukraine, Crimea, and we ended up with occupation. As a response, the European Union put on paper financial sanctions. Let me tell you about Dmitry Kiselyov who was appointed by Putin as Director of the Russian Media Mechanism, a hybrid war mechanism. Kiselyov is the Director of Russia Today or Russia Segodnya and Sputnik. The two are parts of the same system - some of you may recognize it. I searched online and found out that Iceland does not have a local Sputnik web channel as a lot of the countries in Europe do. Many countries outside of Europe also have this channel, trying to look like a regular news channel but is very specifically connected to Russian state-controlled media. To cut a long story short, Dmitry Kiselyov was put under sanctions, which means all of his business, including Russia Segodnya, the big parent company, which means that everything that falls under that is under sanctions. Economic transactions are to be frozen within the European Union. This is what the sanctions entail.

„As I said there are four things in the hybrid definition we need to look at. They try to undermine our trust in democratic institutions, they try to question our societal values, they try to gain political influence and they try to affect decision making.“

As I said before, there is a Sputnik channel in Estonia. The Sputnik case I am talking about started in 2014, when the sanctions were put on paper. In 2015, a commercial bank in Estonia figured out that there was a bank account connected to Russia Segodnya. The account was under control of Dmitry Kiselyov so the account was frozen in 2015. There was no reaction to that. If we now take a big step forward, to October 2019, another Estonian commercial bank discovered that the local branch of the Russian media, the Sputnik, was getting funding from a bank account which was funded by another bank account until the chain was eventually connected to Russia Segodnya and thereby to Dmitry Kiselyov, the person

under sanction. Those transactions were blocked, no reaction. In November 2019, Sputnik was unable to pay rent for their office, because their transactions had been frozen. Still no reaction.

In December 2019, the Estonian government, through the financial intelligence unit, notified the Sputnik team in Estonia, about all of this, because you should be aware that if you work for Sputnik, you work for Russia Segodnya, which is a problem because Russia Segodnya is controlled by Dmitry Kiselyov, who is under the EU sanctions. This is when they saw an opportunity. In December, Putin had his annual

press conference and the narrative of how the Estonian state harasses journalists in Estonia was a topic in the press conference. There was a complaint to the OSCE, that said “look what is going on in Estonia, the state is harassing journalists”. There was diplomatic correspondence taking place between Christmas and New Year, which is when the Western culture is on a lower gear, but the Russian Orthodox culture is not. This was therefore the perfect opportunity to start bombardment of information.

The result of this campaign, what we discovered, was that there had been a tweet by the OSCE media representative, where he refers to a letter he wrote to the Estonian authorities about some issues. They attempted to affect the image of Estonia. Our image is something that is important to us, so we felt we had to clean this up. Secondly, the Russian speaking media, from mid-December until the end of January, posted 1400 news pieces about Sputnik Estonia, the coverage was only negative, nothing positive about it, from very high ranked spokespeople, even the president himself. Nonetheless, there was very low social media reach, as far as we could see. That means that the topic was un-organic. People didn't talk about it. Only the media in Russia wanted to talk about it. The Western media and real media sources, on the other hand, posted less than ten pieces about this. This means that we must be looking at an information campaign.

What are the results, if we go back to the definition of hybrid threats? As I said there are four things in the hybrid definition we need to look at. They try to undermine our trust in democratic institutions, they try to question our societal values, they try to gain political influence and they try to affect decision making. First, they tried to undermine the trust in democratic institutions by putting out a narrative about media freedom. They didn't talk about Ukraine; they didn't talk about sanctions. The narrative was about media freedom. This is a value of great importance to us. We take a lot of pride in Estonia being very high up on the media freedom index. They shifted the focus, pushed the narrative, attacked our trust in democratic institutions and questioned our values. Secondly, looking at political or geopolitical influence. The idea behind the campaign might have been to question the sanctions as such. Again, using the information campaign to reach goals desirable to them. Finally, we come to affecting decision making. The whole information campaign hit at the weakest time of the year, when everybody was on holidays. A tweet was tweeted on 21 December, which means that everyone in Brussels is on their holidays, most people in Estonia are on their holidays and then this thing started to roll. They tried to affect our decision making by overwhelming us, keeping us 2 or 3 or 4 steps behind, making us clean up.

All considered, we were resilient in this situation because of situational awareness, we were capable of detecting this information campaign, seeing the amount of information that was put up by the Russian state media, and state controlled media in the west and also what was happening on social media. We detected it but we didn't react to it, the result is that the EU sanctions are still active and are still being put to use in Estonia and the whole of the European Union.

Thank you.

Discussions

Moderator: **Sveinn H. Guðmarsson**, Press Officer, Ministry for Foreign Affairs

Panelists: **Jurgen Klemm**, Strategic Communication Advisor, Estonian Government Office, **Elfa Ýr Gylfadóttir**, Director, Icelandic Media Commission, **Ingólfur Bjarni Sigfússon**, Senior Correspondent, The Icelandic National Broadcasting Service, **Þór Mattíasson**, Expert in Analytics and Search Engine Marketing, Co-Owner of Svartigaldur

Three main themes emerged from the discussions in session two. They are: 1) Hybrid mechanism and the weaponization of social media 2) Trust 3) COVID-19 and misinformation.

This discussion summary is supposed to give an overview of the debate in the panel and not represent individual views and opinions of participants.

Hybrid Mechanism and the Weaponization of Social Media

It was pointed out by the participants in this session that the Icelandic mentality makes the nation more vulnerable, first of all the notion that Iceland is an island and out of harm's way and secondly that many people believe that they have nothing to hide. The fact is that Icelanders are very well connected, use social media a lot and are being micro targeted all the time. Many people don't realize (or don't care) that every second spent on a social media platform is a second paid to that platform.

Social media platforms and search engines can be weaponized, and that has already happened. Elections are probably the best example where much of the hybrid mechanism taking place goes under the radar, creating chaos and the image that something is out of order.

One of the things that make hybrid warfare so hard to deal with is that it is not always so visible to those who don't know what to look for. Often one could

even question if it was really an attack or if it would fall in a grey area, the attack can be very difficult to pinpoint. The hybrid attack can also be from both foreign and domestic aggressors. That is what makes this method both so dangerous and effective.

It takes a long time to build up the experience and know how to recognize the patterns and gain the confidence to point out an information campaign and know when it is necessary to react to an information campaign. This can only be learned by experience in analysis. It is also very important to educate the public, to teach children to detect false information, to teach and train everyone in media literacy. It is important that everyone understands that the more a person engages on a social media platform, the better understanding the platform builds about who they are, what are their interests and how they function in society. People are offering answers to questions without answering them directly.

Trust

Participants furthermore emphasised the need for more research in Iceland on how disinformation is spreading, leading to diminishing trust. In Iceland, like the other Nordic countries, trust has generally been high, therefore there is much to lose. Iceland is also a close-knit society where trust is an important part of making daily life function. If that can be eroded it takes a long time to repair.

It seems to be more common that the older generation is less used to having to discern if the information they are using is credible or not than the younger generation. Kids and young adults are used to detecting fake information online, i.e. they recognize a fake URL, while the older generation reads something online and often assumes that it must be true.

A few suggestions were brought up about what could be done. Philosophy could be introduced at an earlier age in schools as well as media literacy and critical thinking. Technology is changing and advancing very fast, therefore the public needs to be prepared to look critically at new technology before adapting to it.

Election interference is very interesting in the hybrid context and raises challenging questions like what would happen if a deep fake of a politician would go out 48 hours before elections? In many states in Europe this would be during a so-called dark period before elections when the media isn't even allowed to say anything. The media environment has changed dramatically in accordance with how fast information spreads through social media. Some mainstream media outlets have launched platforms or sub platforms to correct errors and fake news or whatever may be reported by other media channels. The media has always had to deal with people pushing narratives based on their interest, they are used to check facts in order to get them straight. In the new media environment these interests can go under the radar. Anyone can micro target their audience and push their narratives towards them.

Another challenge for the media environment is that there are still old-fashioned laws on traditional media but nothing on social media - where much is happening. If the law is outdated, it can even be harmful, preventing the mainstream media from distributing the right information during this critical time period prior to elections.

Important questions to ask at this point include which governmental institutions should be involved in fighting hybrid threats and attacks? How should they do it? What kind of research is needed? What kind of cooperation is needed? Who should have the task of coordinating all that? Given the complexity of hybrid threats it is very difficult to say that a certain model should always be used, it has to be decided on a case to case basis following an analysis of the problem.

COVID-19 and Misinformation

The participants also connected the topic to COVID-19 which could prove to be a live exercise in detecting hybrid campaigns. There is a lot of false information and even conspiracy theories online and misinformation about the coronavirus which may even be spreading faster than the virus itself. Those who are really scared may be more willing to at least entertain the possibility that there was some truth to it, wondering if the government is actually telling the whole story.

Although fake news and disinformation may not be very obvious in Icelandic discourse, Iceland is no exception from this. False narratives are being pushed all the time.

3.

Third Panel Session:

Importance of Fostering Resilience

Moderator:

Svana Helen Björnsdóttir,

President of the Association of Chartered Engineers in Iceland.



Flemming Spildsboel Hansen,
*Senior Researcher, International Security,
Danish Institute of International Studies*

Thank you for the invitation to join you here today and share my perspectives, partly from Denmark but also more general on the importance of fostering resilience.

As we have already learned here today, we are discussing very complex threats. We live in very complex times so the answer, unfortunately I expect, will also be very complex. I will talk about resilience in times of weaponization. You have already heard of some of these issues and concepts. I will also focus on resilience and weaponization. No one has really defined the terms yet, but they are difficult to deal with and also to implement. Much of my work is on information operations and disinformation is a part of that. I suspect that we will continue to see more advanced information operations in the future, making it even more difficult for us to detect and deal with.

In the work I do right now, I focus on three domains, a physical domain, digital domain and cognitive domain. You may have heard about the digital domain more often referred to as a cyber domain. I like to use the term digital domain because it reminds us that this is where we have our critical digital infrastructure. This has already been somewhat discussed here today for instance how we get hacked and how some of the systems we rely on for payments may be compromised. Then we have the cognitive domain which is where the thinking takes part. The cognitive domain is the target of disinformation campaigns, to try to influence people to vote in a particular way for instance. A lot of the work I do right now and what I suspect some of you will find particularly interesting is the relationship between the digital and cognitive domains. The way I like to describe it is as a kind of big bang within those domains. We have a big bang within the digital domain or the cyber domain. New technology as we have already discussed, Nora for instance talked about artificial intelligence and the ways it enables actors to collect, process and use more information, advancing the ways to influence voters. There is also a kind of big bang within the cognitive domain. It's much less dramatic but it's there as we know much more today about how to influence people to behave in a particular way than we did just a couple of decades ago. Within psychology there have been studies and great advancements on how to influence behaviour and particularly suboptimal behaviour, getting people to make stupid decisions.

Now I will attempt to define weaponization, which is a great term. I really like it because it reminds us of the fact that certain assets may be used to achieve certain objectives.

Actors think instrumentally about how they can use this particular asset to achieve their goals. At the same time the term is also problematic since everything today can and is being weaponized, so it loses part of its content. Here is an example:

„Hybrid threats are nearly all-encompassing, unfortunately so is the response. Almost every type of threat that we can think of, at least in combination with something else can be considered a hybrid threat.“



Weaponization as the use of assets within the domains with the purpose of creating political, strategic, operational, or tactical effects in support of policy objectives.

Antonio talked about the kinetic threshold and how weaponization is often thought of as the extramental use of non-kinetic assets. These are the assets you will find within the digital- and cognitive domains, for instance how social media can be used to achieve certain purposes. In the previous session we learned how to weaponize social media and the digital critical infrastructure in order to impose damages.

But weaponization can also happen within the physical domain, where ordinary things like cars, have been weaponized. Cars are a good example of an asset that most of us have and can be turned into a weapon. Both weaponization and resilience are terms we need to consider in all three domains. Just as assets may be weaponized within all three domains, we must foster resilience within all three domains.

I want to draw your attention to the interplay of the digital and cognitive domains. Most of the discussion we have had today have started out being fairly broad, about almost everything, and then narrowed down to disinformation because that is something we can handle. It is a challenge for us to deal with all three domains at the same time, both in terms of threats emanating from them and resilience. Even if it can be good and useful to focus on disinformation, we need to keep in mind that hybrid threats are broader and more ambitious, making the challenge more difficult.

The whole session here today is on hybrid threats, and hybrid threats is also both a great term and a problematic one. As the prime minister mentioned in her welcoming address this afternoon, there is a risk that the term becomes fuzzy, that we lose the sense of what it is. Some of the examples we have heard today are already on the periphery of what could be considered hybrid threats. If you look back tonight and review some of the things that have been said today, I expect that you will understand that the hybrid toolbox really contains quite a lot and that some of the examples we heard today are on the periphery. Nonetheless, we should have a better understanding of the way actors may think.

Hybrid threats are nearly all-encompassing, unfortunately so is the response. Almost every type of threat that we can think of, at least in combination with something else can be considered a hybrid threat. Here is an example of a definition of resilience by the EU Commission (2017):

- **The adaptability of states, societies, communities and individuals to political, economic, environmental, demographic or social pressures (...)**
- **The capacity of a state – in the face of significant pressures to build, maintain or restore its core functions, and basic social and political cohesion (...)**

It mentions adaptability, societies under pressure, states under pressure and the ability to build and maintain and restore core functions and basic political cohesion. The previous speakers talked about social cohesion, a very important topic, which brings us back to the cognitive domain. How we can deal with these threats, and how to enhance people's understanding of the concept and value of democracy and freedom of speech and what it means being Icelandic for an example. Threats can occur within all three domains, so it is necessary to build and strengthen resilience within all three domains as well. Strong focus has been on the cognitive domain and political thinking, the cohesiveness that you will find within societies.

If we accept that this is a very complex threat, ranging from the physical, on to the digital, and finally the cognitive domain then we need to focus on resilience within all three domains and face some difficult questions such as:

- **How do we prioritise with limited spending?**
- **To what extent should restrictions be imposed?**
- **How far should surveillance be rolled out?**
- **How should public and private responsibilities be divided or shared?**
- **How do we manage tenders, mergers and acquisitions?**

How do we prioritize? Given that we have three domains and that we are facing threats under all three domains, how do we deal with limited spending? What do we prioritize, where do we put our money? We are familiar with anti-terrorism resilience. Most of us, or all of us probably as we travelled to the university were confronted with counter terrorism, resilience measures, even if we didn't see them, didn't recognize them. But they are in place. Especially for those of us who came from abroad. They are expensive and drain some of the resources.

To what extent should restrictions be imposed? This applies both to freedom of movement and freedom of speech. Some of the challenges have already been discussed today. Denmark for instance found a need to revise its anti-espionage legislation in view of possible cooperation between people in Denmark and users of outlets that are controlled by foreign states. This was very controversial but also seen as necessary, for us to update the anti-espionage legislation in light of developments within social media. A majority of parliamentarians found this very problematic but at the same time absolutely necessary.

What about surveillance? We all enjoy surveillance, but we are also very critical of it and some of the surveillance of course will be online. Where do we draw the line between what is acceptable for security services to monitor, store and analyse and the freedom of speech? This is a discussion that is taking place in my own state, Denmark.

Another important question relates to the division of public and private responsibilities. Whose responsibility is this? A while back I was doing a presentation for the director of the Danish Centre for Cyber Security, which falls under the Danish intelligence service. When I was speaking about how to protect yourself within the digital domain it became clear from the reactions from the big industries and companies in Denmark who were represented at the meeting, that if something was to happen, they could call him. But he said that they would have to go through the private sector. How can we ensure cooperation between the private and public sectors?

Now to the last question, how do we manage tenders, mergers and acquisitions? I was in the Faroe Islands just last week and they are still very concerned about Huawei and 5G, the new network, because the Danish government said that they cannot go to Huawei. Who should they do business with, why can't they go to Huawei and who will compensate them for their losses? These are very big and very difficult questions.

Thank you.



Kristi Narinen,
*Director of International Relations,
European Centre of Excellence for Countering Hybrid Threats*

Dear all, thank you very much for the invitation. This is my first time in Iceland, and I hope that soon Iceland will become a part of the Hybrid Center since that would complete the NB8, which is one of my favourite concepts.

I would like to start with looking at this Zero-One world which is the conceptual environment we grew up with during the Cold War. Fact-Fiction, War-Peace, Private-Public, Military-Civil, Internal-External, Friends-Enemies. All these were clear divisions, but the structure is changing, the edges are blurring and even fading away. Our task now is to make at least a part of this Zero-One world remain, Fact-Fiction etc. and this is what it is all about.

Hybrid threats have already been described here today, but I would still like to summarize how the Center of Excellence defines them. There are three elements hybrid threats comprise of:

- **Coordinated and synchronized action, that targets democratic states' and institutions systemic vulnerabilities, through a wide range of means.**
- **Exploit the thresholds of detection and attribution of war and peace, internal and external, military and civil, public and private.**
- **The aim is to influence decision making at the local (regional), state, or institutional level to favour and/or gain the agents strategic goals while undermining and/or hurting the target.**

The measures are not always particularly coordinated or synchronized, and not always strategic, aggressors can also take advantage of an opportunity offered, for instance by a natural disaster or political processes. If you are a visual person like I am you would probably notice in our logo that we connect the red dots, the negative maligned action into one entity. Those can be several activities of different character within one country, or they can be similar elements cross borders, or both. Joining them makes this concerted action, hybrid.

Blurring the binary world, exploiting the threshold, both detection and attribution, has been mentioned here several times, so has targeting the decision making, so I'm luckily not saying something that was not said before. We risk making the wrong decision if we don't detect what is happening since that will benefit the strategic aim of the adverse, which are always contextual. Because one operation in one country is not necessarily the same as in another one. Even if you analyse the NB8 and N5, you find differences in the value-based context, for instance political history, economy, political system etc.

Today's theme is resilience, so what does it mean to be resilient? Is it about resilience to endure, or resilience to deter? For instance, Sputnik opened offices in Sweden and Finland, but closed quite quickly because there was no market base for that.

Or perhaps resilience to revive, this was also described earlier. We have to consider the meaning of resilience. In the Hybrid CoE, our structure resilience is connected with vulnerabilities. Here you see a collection of elements that I would like to explore in the context of a bigger picture:

- **Democracy**
- **Democratic institutions**
- **Human rights (social obligations?)**
- **Market economy**
- **Freedom of speech**
- **Free media**
- **Rule of law**
- **Civil society**
- **Trust to state structures and authorities**

These are the building blocks of society, our freedoms, obligations, values and interests. It's in our interest to have the freedom of speech, or the freedom of expression. Things that we in the Nordic family have and are making us the most resilient states in the world. These are the strongholds of resilience.

If you turn the logic around, deficiencies in these elements might become a vulnerability and we can be absolutely certain that the adversaries and opponents are mapping our societies as we speak. They are already finding our vulnerabilities and weak spots and are sneaking into our societies through these vulnerable gates. If we don't see them, we need to listen to the squeaking doors through which they are entering, we have to smell, and we have to feel. We also have to remember that they are very quick in learning how to oil the hinges, so even if we hear them now, we might not hear them later. To be able to use all the senses we have, we have to develop a better understanding of the theme, the awareness raising, which was mentioned earlier, better understanding of down streams in our own society. We must also think slower and exercise critical thinking, more facts and analysis, less emotions and conspiracy theories.

„Hybrid threats call for joined efforts and responses. It requires strategic thinking and political will to be intellectually honest, even when it is politically difficult.“

International cooperation is of great importance here, first of all international cooperation can enhance communication and trust, it can help identify the activities and the platforms so that we can discuss and share them. The key is to look far and act near. By now we have realized that we need new skills, attitudes and visions of admiring the problem, which is quite often done. However, building resilience and any other defensive action is not the duty of one, or even a few. Hybrid threats call for joined efforts and responses. It requires strategic thinking and political will to be intellectually honest, even when it is politically difficult. In the European security debate government actions are relatively widely accepted, but that is not sufficient. We need the civil society and the private sector to play along, action needs to be taken in the whole society.

Critical infrastructure for instance is often handled by private companies yet providing public service. Critical infrastructure resilience also means interoperability, we did research on this. We need to look at critical infrastructure from the user's perspec-

tive, we tend to focus on the service provider's perspective. For example, if we have a case of a power cut, hospitals have generators, so they can provide electricity, but if the water supply system is also out, there is not a lot that you can do in a hospital that has electricity, but no water.

If the citizens feel safe, the trust estate structure is strong which is what the society needs. It is also what the adversaries are trying to diminish. Therefore, every citizen is needed to enhance resilience, everyone is responsible and should use strong passwords, check the information and facts from several sources and think slowly. The human mind is actually probably the sixth domain, which was described earlier in the cognitive thinking. Another important factor is strategic communication of the authorities themselves; they must be well-structured because we need to tell our narratives before somebody else does, just like the Estonian example showed us.

Another thing I would like to mention about the Nordic system which makes it particularly resilient, and that is the low organizational hierarchy. As Hybrid operations are usually abnormalities in the society, they are often detected at the grassroots level. If reporting upwards functions well, the detection leads to action a lot faster than in systems that require more formalities. The rule of law system is also one element of resilience, both the law itself and the ability to enforce them, this applies not only to the existing legislation but also to changing circumstances requiring will to pass new laws, where the viewpoint regulation might be unforeseeable, or even weird. Legal resilience must breathe with the pulse of the surroundings.

Now just a few words about the Hybrid CoE. The centre started only three years ago, and has already achieved quite a visible position both in terms of brand and agenda in the European transatlantic security landscape. There are twenty-seven participating states, they are all EU and/or NATO members, and EU and NATO offer the platforms to discuss, identify, take action and counter the threats. The centre is a do tank actually, rather than a think tank. It brings in experts, particularly cross-institution experts, to engage in discussions, teaching and learning. In other words, if you organise a meeting where only people from the military are invited to talk about military perspectives, the most likely outcome will be military, the same applies to lawyers, politicians, business, finance etc. and also the media. When we bring experts from various sectors together, that is the format likely to deliver something new, innovative and useful. The Hybrid CoE wants to be the leading conversation handler, for which it has a fair chance as it doesn't have its own agenda, there are no political constraints and no obligation of consensus.

To conclude, we need to be aware of the risks, we have the tools to identify, we have our own existing approach to vulnerabilities and building resilience, but only if we exercise slow thinking and intellectually honest analysis. We also need to realize that this is a time to act. We need each other and the international community along with the eight partners. Our allies are thinking about the same challenges but not all draw the same conclusions, however most of them do. Our opponents on the other hand want us to think that we need them to solve our problem. Actually, we are quite capable of handling the challenges ourselves, but not alone. With friends it's much more fun.

Discussions

*Moderator: **Svana Helen Björnsdóttir**, President of the Association of Chartered Engineers in Iceland*

*Panelists: **Flemming Spildsboel Hansen**, Senior Researcher, International Security, Danish Institute of International Affairs, **Kirsti Narinen**, Director of International Relations, European Centre of Excellence for Countering Hybrid Threats, **Bergur Ebby Benediktsson**, Author and Societal Analyst, **Hrefna Sigurjónsdóttir**, Director, Home and School – The National Parents Association, **Hákon L. Akelund**, Specialist in Cyber Security, Landsbankinn*

Three main themes emerged from the discussions following the speeches in session three. They are: 1) Resilience 2) Values 3) International collaboration.

This discussion summary is supposed to give an overview of the debate in the panel and not represent individual views and opinions of participants.

Resilience

The participants pointed out that resilience can be defined and interpreted in many ways, including:

- a) In the terms of well-being on the individual level, mental and physical health, succeeding in life, work, education etc.
- b) As the capacity to recover quickly from difficulties, the ability to spring back into shape.
- c) As both toughness and adaptability. Toughness is sometimes considered more old warfare while becoming more adaptable is considered necessary for future generations.

Furthermore, resilience should be fostered throughout the school system as well as public awareness raising, it concerns everyone, the media, political parties, organizations and institutions. Since it concerns everybody, a holistic approach is needed. There is no cause for panic but that is not to say that this is an easy task, it is not. It is also a task that doesn't have an ending, it will not go away. It is a learning race

where the aggressors will always be one step ahead. Just like with international terrorism people will learn how to deal with hybrid threats.

The main obstacles to resilience and awareness are the social media platforms and more in general the IT culture which has a value system encouraging the opposite of resilience. The users are encouraged to be open, even vulnerable, which is also a generational global trend, not only in technology. The openness makes it harder to counter the threats, especially with conventional methods and it becomes more important to deliver the message not only through core education with subjects but also with all the extra-curricular activities. We all have to understand that the chain is only as strong as its weakest link.

Values

One of the topics that the participants brought up during the discussions is values, what is it actually that we are protecting? Should we place a stronger focus on the values we want to safeguard for future generations, rather than on the threats?

Terminology was also discussed and the definition of disinformation which is "information that strategically is implying something false. False information". However, by applying critical thinking one could come to the conclusion that disinformation is not a real concept, by assuming disinformation gives out something that is false we are saying that information has

value. But information does not have value. According to basic information theory information is neither good nor bad, information is about things that have value.

In regard to values a good education and a strong knowledge base are cornerstones, but in modern education there is still need for fostering better initiative and critical thinking, digital citizenship and media literacy. This applies both for children and in adult learning. This should be emphasized in the new education policy that is being developed in Iceland and will last until 2030, in the chapter on digital citizenship and media literacy. These values and interests should constantly be implemented and thought of and never taken for granted.

Narratives are constantly being pushed towards us all and trust is very important to counter these narratives. Propaganda is not new but the ways to spread it are completely different and much faster than before. This needs to be taken into account when plans for the education system are being made. It is of utmost importance for governmental bodies to gain or regain trust and show the public that they can be trusted. If the aim is to make citizens and not just consumers, digital citizenship and media literacy must be looked into and the government has to be trustworthy.

Finland, Sweden, Estonia and Latvia have developed and implemented national resilience programs for elections, and this could be valuable for other election committees. One of the elements in the program is focused on how to get young people to vote and how to get people to vote based on ideologies, principles, facts and figures rather than emotions and quick- and superficial responses. That is what democracy is all about and that is where politicians also have a challenge.

International Collaboration

Finally, the panel participants raised the issue of the law in Iceland and how far it is from being sufficient when it comes to handling the incidents, we see in the financial world today. To be better able to handle cyber incidents it is important to act fast, share information about possible threats and ongoing attacks or aggressions. Both Nordic and European cross-border cooperation has proven to be beneficial in these regards. Nonetheless, Iceland has a far way to go to catch up with the other Nordic countries and active involvement is needed from the legislators, public- and private sectors and by the whole community.

The participants agreed that international collaboration is crucial for sharing best practices and learning new ways to raise awareness, prepare and educate citizens in media literacy. Even if there is a lot to be learned by international collaboration, the case is still that by using Icelandic examples about data leaks from organizations or private persons to educate citizens, they gain a much better understanding, both from people and organizations about what was happening. It is easier for people to take in information they can adapt to.



Closing Remarks

Silja Dögg Gunnarsdóttir,
President of the Nordic Council

Dear guests,

I want to start by thanking all of those who have collaborated with the National Security Council in organizing and contributing to today's conference and for making such an interesting and timely conference. There have been many noteworthy contributions here today that are not easy to summarize.

A few that struck me, in no particular order, concern the use of personal data, data privacy, data flow and how easy it is to gather personal data legally. Also, the importance of awareness and critical thinking to protect the Nordic gold, that is the trust which we base our democratic societies on. Like Elfa Ýr Gylfadóttir said earlier today, we cannot afford to lose this trust, so we have to stand tall and protect it. It seems very clear to me that we need creativity and initiative while safeguarding our democratic values in addressing the hybrid challenges that we face. Accordingly, it is wonderfully refreshing to see a conference such as this one, exploring new ideas and providing progressive thinking in support of engaging all sectors of societies in our efforts. In order to explain why this is not just relevant and important for the work I do; I need to briefly tell you about what the Nordic Council is and how it works. I know that many of you already know this, but some might not.

The Nordic Council is a platform or a forum for parliamentary cooperation in the Nordic countries. The Council consists of 87 parliamentarians from the Nordic countries, also including Greenland, Faroe Islands and Aland Islands, and reflects the national parliaments in the sense that the proportion of country votes for each party dictates how many representatives they have in the Nordic Council.

I think it is important to explain in a few words how this works as it is different from the national parliaments. Like the national parliaments, our role is to make resolutions for changes and point out areas in need of change. These resolutions and suggestions get forwarded to the Nordic Council of Ministers, the cooperation forum for the Nordic governments. It consists of 11 councils led by the national ministers of the relevant policy area and just like on the national level it is their responsibility to execute the resolutions and proposals we hand them if they want to. Unlike on the national level, the Nordic Council of Ministers is not obliged to act on the sugges-

tions made to them. The presidency of the Nordic Council rotates between the five member states and this year Iceland holds it. In brief that means that the chair of the Icelandic delegation, in this case me, is also the president of the Nordic Council of Ministers. Furthermore, this means that the annual session will take place in Iceland later this year, in Harpa in October. Last but not least it means that we are in charge of the agenda, for the most part.

We have chosen three priorities that we want to work with this year, these are:

- Promotion of the Nordic language skills
- Standing up for biodiversity
- And most importantly in the context of today's conference, combatting information chaos and fake news

These priorities shape our work this year as well as the work and focus of many other institutions around the Nordic countries. We will work with these priorities by promoting awareness through conferences, debates, seminars, articles and more. At the end of March, for example, at the end of the Nordic Council's next meeting in Helsinki, the theme will be disinformation as a threat to the Nordic model. We will discuss how to protect democracy and how to stand up against fake news which undermines it. In May, the Nordic Council, Baltic Assembly, and the BENELUX parliament are arranging a trilateral conference entitled Comprehensive Security and Defence Cooperation: Shifting Landscape and Joining Forces, where we will talk about hybrid threats and warfare, defence cooperation and cyber security, amongst other things. I will participate along with my colleagues and vice president of the Nordic Council, Oddný Harðardóttir. This conference is not just relevant for us as representatives of the Nordic Council, but also on a more direct level relating to our Icelandic work, since we happen to be the only two parliamentarians representing the National Security Council of Iceland. In addition to these events, we aim to strengthen professional and reliable media outlets and journalists by providing relevant courses, promoting their work, and helping people disengage from media that is engaged in distributing disinformation and undermining democracy, for example by provoking hate speech.

All of this is the reason why I really appreciate everything that has been said here today, and all the lessons learned. We chose fake news as a threat to democracy as a focus area for a reason. This conference is also held for that very same reason. We are facing a threat, a real one, and we all need to work together to counter it, not only by discussing things, we also need to take more actions.

I want to end this by thanking again everyone for the inspiration and the knowledge you have shared. I for one, have learned a lot that I will make further use of in the fight against hybrid threats and threats to democracy. Thank you for today and I hope to see you again someday.

