friends of europe

WINTER 2018

HYBRID AND TRANSNATIONAL THREATS

CAN EUROPE TURN THE TABLES ON HYBRID WARFARE TACTICS?

EVENT REPORT

With the support of

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

TABLE OF CONTENTS

NEW THREATS, NEW REALITY

How can Europe work together to turn relatively low-risk, high-gain hybrid warfare activities like cyber-attacks, election interference, fake news and disinformation campaigns into a low-gain, higher-risk venture for its adversaries?

This was among the many questions addressed at a Friends of Europe debate on Hybrid and Transnational Threats, held in Brussels on 5 December, at which a new discussion paper on the same topic was launched.

Moderator and Friends of Europe Senior Fellow, Jamie Shea, cautioned that ahead of the European Parliament elections in May 2019, it would be crucial to "come to grips with where we are, what we're doing well and what we need to do better".

Panel member, Clare Roberts, Senior Policy Co-ordinator for Hybrid Warfare and Resilience at NATO's Operations Division, said that their priorities included enhancing the ability to recognise and attribute hybrid warfare, as well as strengthening resilience through exercises and training.

MEP Urmas Paet, rapporteur of the 2018 Cyber Defence Report, said more cyber security experts were urgently needed, warning that 'fake news' posed a serious threat because it changes political realities while remaining stubbornly difficult to act upon.

Head of Facebook's Brussels office, Thomas Myrup Kristensen, said that the social media giant had stepped up their game on safety and security issues by hiring 20,000 new people committed to preserving them, in addition to blocking around 2 million fake accounts daily.

WHAT'S THE PROBLEM?

Designed to create confusion, sow discord, exploit fear, disable vital systems and disrupt 'norms' with impunity, hybrid threats are, by their very nature, challenging to predict and counteract.

With aggressors' ever-increasing ability to shape-shift and attack from a myriad of angles, the necessity to face down these threats through cooperation between EU and NATO member states – as well as between national government departments and the private sector – has become all the more important.

This subject has been the topic of an "agonising debate" in recent years, noted Jamie Shea, as he opened the debate and discussion paper launch.

WHAT ARE HYBRID THREATS?

Given how the subject dominated the political zeitgeist in the period following the 2017 US elections, the threat of election interference as a non-military act of aggression by a foreign state is a very real one now that the European Parliament elections are looming.

But there are many elements to hybrid warfare, according to Shea, who identifies three main categories, from which confusion often arises:

1. "The legal type": Is the Chinese ownership of EU ports, or the airing of a Russian news station on European TVs a hybrid threat or "just globalisation?", he asked.

"Should we have a sense in Europe that we need to dominate a larger part of our defence technology and industrial base?"

2. "The daily illegal acts": Including election interference, 'fake news', cyber attacks, and staged provocations, like the use of the nerve agent Novichok in the UK – "it's hostile activity but is below [NATO's] Article 5 level… so do we just let it happen?"

3. "The prelude to a military attack": As seen in Crimea in 2014, this type of hybrid activity is the first phase of an act of aggression, "but how do we deal with that?," asked Shea.

Tackling these multiple threats requires multiple tactics and strong partnerships, but ultimately, "modern deterrence is by resilience," said NATO's Clare Roberts.

ARE WE WORKING TOGETHER WELL TO INCREASE RESILIENCE?

Countering hybrid threats is primarily a national responsibility, NATO's Clare Roberts reminded participants, but the alliance is working to boost resilience and cooperation.

The fact that it's still a national responsibility is a "serious problem," warned former Estonian Foreign Minister, Urmas Paet, who said: "We are very dependent on the weakest link."

Jamie Shea highlighted joint initiatives like the PESCO project for EU Cyber Rapid Response Force teams and asked if more should be developed.

Facebook's Thomas Myrup Kristensen said governments, security specialists and tech companies were learning from each other, but cautioned that the "arms race" would continue in the long term.

Roberts said hybrid warfare was a "top priority" for NATO: "[It] is a reality. It confronts allies pretty much on a daily basis," she said.

"We are very dependent on the weakest link."

Urmas Paet
Former Estonian Foreign Minister

1.

2.

1. **Jamie Shea; Thomas Myrup Kristensen,** Managing Director EU Affairs and Head of Brussels office at Facebook**; Clare Roberts,** NATO**; Urmas Paet,** Member of EU Parliament

2. **Paul Mitcham**, Political Advisor, European External Action Service (EEAS) EU NAVFOR

3. **Chris Kremidas**, J9 Interagency Liaison to NATO, EU, and OSCE, U.S. European Command (USEUCOM)

3.

4.

5.

4. **Jamie Shea, Kris Kremidas, Geert Cami, Geert Cami,** Co-Founder & Secretary General at Friends of Europe.

5. **Ana Alvarez Roldan**, European Parliament Directorate General for External Policies; **Nuria Martin Guardiola**, Security and Defence Policy Analyst, European Parliament DG EXPO

“We want free and fair elections as well, we want correct information to get to our users, and to be a platform that contributes positively to societal debate.”

Thomas Myrup Kristensen
Director for EU Affairs and Head of Facebook’s Brussels office

She said the alliance was working on all three elements needed – to prepare, deter, and defend against these threats.

Preparation work would include building the ability to recognise and attribute hybrid threats and urging nations to come forward with information on threats they faced. NATO had also been putting members through exercises and training on responses, as well as working to increase resilience in vulnerable strategic civilian sectors.

“Good resilience is a good immune system to many of these threats,” she said.

A “whole of government approach” was crucial, she said, acknowledging ministries such as transport, health, energy and communications, as well as the private sector.

“On the ‘deter part’ you have to get the balance right. NATO is very much a defensive alliance so, to an extent, we are on the back foot a lot of the time.”

She said one new “tool” was NATO’s Counter Hybrid Support Teams, which dispatches experts at an ally’s request.

NATO had also been working with the EU, said Roberts, through the distribution of playbooks, increased staff-to-staff cooperation, and learning from “robust, whole of government, resilience systems” in Finland and Sweden and from hybrid threat victims like Ukraine.

DISINFORMATION AND THE EU ELECTIONS

Looking ahead to the European Parliament elections, Jamie Shea asked Facebook’s Thomas Myrup Kristensen what lessons had been learned on ‘fake news’ and disinformation during the 2017 US elections.

In addition to being responsible for the adoption of new measures at Facebook, there was now “greater interaction with national intelligence services or government services”, said Shea, who questioned whether or not this symbolised a permanent relationship.

“I think that partnership is actually really essential to deal with this,” said Kristensen.

“We have a lot of experience from the US elections, but also from European elections. We worked with Germany when there were elections there, and in France, Italy and Sweden recently. For the European Parliament elections, our aim is to work with all 27 countries.

“We want free and fair elections as well, we want correct information to get to our users, and to be a platform that contributes positively to societal debate,” he said.

He said that Facebook's strategy had included hiring 20,000 new people to work on overall safety and security issues, and that their 'real name' policy was "key".

The use of fake accounts to generate 'viral' activity around a piece of 'news' was an often-employed tactic, he said, but a resulting crackdown had led to around 2 million fake accounts being pre-emptively shut down every day.

On the subject of fake news, he singled out one particular challenge: "We have to balance out freedom of expression with the spreading of misinformation."

He said Facebook was not established to be "the arbiters of the truth", so they had engaged third party fact-checkers to review information and reduce the distribution of false materials.

WHERE ARE THE GAPS IN OUR RESILIENCE?

Discussion points ranged from tackling wider societal issues, to more tangible recommendations, such as increasing the number of cyber experts.

In response to a question on whether the 'gilets jaunes' protests had been "hijacked by other forces", one of the discussion paper authors, Chris Kremidas, said it wasn't yet clear but the question was a legitimate one.

"One of the easiest ways for a hostile state actor to employ a hybrid type of approach is to take existing societal and historical wounds, and situations and tensions, and poke their finger in try to amplify them or make them a bit messier."

Cyber attacks represent one of the most dangerous threats because attacks against nuclear power facilities, aviation control systems, or hospitals, could lead to people dying, said Urmas Paet.

"In Europe, we're missing around 150,000 specialists who can do something about this. It is urgent that our universities and military academies teach more experts in this field," he said.

But he added that we shouldn't underestimate the power of "massive campaigns of lies", which can quickly change public opinion and the political landscape.

One of the most recent large-scale campaigns in Europe was about immigration and refugees, he said, adding that there was "real hysteria going on".

"Part of this is a systematic fake news campaign. In Estonia we have 1.3m people and increasingly people come to me and say 'we saw on Facebook that there is a plan to bring 17m refugees here'. More and more people simply believe this."

"One of the easiest ways for a hostile state actor to employ a hybrid type of approach is to take existing societal and historical wounds, and situations and tensions, and poke their finger in try to amplify them or make them a bit messier."

Chris Kremidas
NATO and Political-Military Expert, Liaison to NATO and EU at US European Command

“Why is it that we’ve got by far the more positive and better story, but the bad guys constantly out-communicate us?”

Jamie Shea
former NATO deputy assistant secretary general for emerging security challenges. Moderator and Friends of Europe Senior Fellow

“This is perhaps one of the most difficult spheres because there is no real action NATO or the EU can take. It’s about our societies, common sense, and the critical mind.

“In Europe there is too high a level of naivety. The new generations, people without their own personal memories of tragic events from the past, are a bit too naive. There should be more of a duty on school systems to teach how to recognise fake news and propaganda, and see the difference between sources of information,” he said.

There should also be concerns about direct propaganda, said Paet, adding there was also naivety about the free broadcasting of TV station, Russia Today, for example.

KEY CONCLUSIONS

Nations need to be less ashamed and more up front about the hybrid threats they’re facing, said Clare Roberts, who urged a “change in mindset”.

Common sense says there should be “100% cooperation, not competition” between the EU and NATO, said Urmas Paet, who said that while more money for security and defence was likely, massive military spending in Europe was not.

“NATO is there. We should concentrate on the practical added value to the EU’s security picture,” he said.

“We need to map all our vulnerabilities, particularly the dependencies between different things, so we don’t have cascading hybrid effects,” said Jamie Shea, the former NATO deputy assistant secretary general for emerging security challenges.

He said his takeaways also included the need to mobilise Europe’s resources and make everything fully accessible to all; train and exercise on responses; recruit and train more specialists; decentralise resilience, for example by learning from city mayors at the coalface; develop resilient citizens and improve the playbook of responses to hybrid attacks.

Improving our “narrative” was also crucial, he added: “Why is it that we’ve got by far the more positive and better story, but the bad guys constantly out-communicate us?”

Hybrid warfare has an “infinite” number of actors and instruments, he said, elaborating with the following view: “We are divided, and therefore are a juicy target, and unfortunately we are not going to be able to heal some of those wounds quickly.”

“But it’s clear that we’re not helpless and we are not sitting back.”

Friends of Europe
Connect. Debate. Change.

+32 2 300 29 92
info@friendsofeurope.org
friendsofeurope.org

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