EUROPEAN
COUNCIL
ON FOREIGN
RELATIONS
ecfr.eu

STRATEGIC SOVEREIGNTY

PROTECTING EUROPE AGAINST HYBRID THREATS

Gustav Gressel

June 2019

SUMMARY

- Geopolitical rivals to Europe are increasingly incorporating hybrid threats into their armouries – and deploying them.
- This amorphous set of threats exists below the level of war, enabling other powers to exploit existing societal divisions and sow confusion and instability.
- To deal with hybrid threats on their own, EU countries will need to more thoroughly investigate such hybrid activities – and go public with their findings.
- Europe should pursue a 'dual track' approach of confrontation followed by dialogue with unfriendly cyber powers.
- EU member states should also jointly invest in offensive cyber capabilities within PESCO, expand Europol's remit to include counter-intelligence, and improve personal cyber hygiene standards in government and among citizens.

On 12 October 1983, Ronald Reagan signed off the top secret National Security Decision Directive 108 on "Soviet Camouflage, Concealment and Deception". The document bluntly stated that:

> *The Soviet Union has developed a doctrine of "maskirovka" which calls for the use of camouflage, concealment and deception (CC&D) in defense-related programs and in the conduct of military operations. They define maskirovka as a set of measures to deceive, or mislead, the enemy with respect to Soviet national security capabilities, actions, and intentions. These measures include concealment, simulation, diversionary actions and disinformation. A Soviet Directorate for strategic maskirovka has been established … Several recent discoveries reveal that the Soviet maskirovka program has enjoyed previously unsuspected success and that it is apparently entering a new and improved phase.*

This quote could easily come straight from a defence white paper of an average NATO member state in 2019. Europe's current geopolitical circumstances are not the first in which it has had to face threats of a "hybrid" nature. They are unlikely to be the last.

The situation may not be wholly new, but it is certainly strained nevertheless. After a decade of economic crisis, Europe's political systems are worn out. Relations are worse than usual among some of the European Union's member states, between Europe and the United States, and between social groups within member states. And it is now cheaper and easier than ever for those wishing to exacerbate those cleavages to do so through cheap social media adverts, a few bots, and a handful of hacks – all backed up with some shady finance schemes. Without relying on the US, can Europe really be sovereign in the face of hybrid threats? This paper assesses how and to what extent the states of the EU can deal with such threats if they have to act alone.

From Trojan horse to Trojan malware: What are 'hybrid threats'?

The term 'hybrid threats' has doubtful conceptual value. Various definitions have attached themselves to it, and other terms compete with it too, such as 'non-linear war', 'asymmetric conflict', and 'subversion'. But, in short, 'hybrid threats' refers to the use of state-sponsored, but not officially affiliated (deniable), actors that do not resort to physical violence. The purpose of hybrid threats is to coerce the object of a threat into complying with the aggressor's strategic interests. There is an implicit warning of the use of force behind such threats. As one EU member state official with the newly bestowed title of "ambassador for hybrid threats" recently told the European Council on Foreign Relations: "There is no such thing as a 'hybrid threat' [on its own]. Hybridity comes into play when threats from various policy fields are fused together."[1]

Hybrid tricks have been used throughout history, from the Trojan horse devised by Odysseus to the Trojan malware written by hackers today. Indeed, even periods of peace are 'hybrid', punctuated as they are by assassinations, corruption, spying, disinformation, manipulation, and economic pressure. Public debate about hybrid threats concentrates on fake news, information warfare, and social media manipulation. This attention is understandable: fake news is the most visible element of a hybrid campaign. But states' means of using undisclosed and unattributed assets to weaken their adversaries go far beyond these elements. And disinformation is rarely an end in itself, but rather a preparatory stage for further subversive action. Extensive intelligence, conspiratorial, and subversive efforts can weaken an opponent's society in a way that allows a foreign power to enter and take advantage of the situation. Most western Europeans were surprised by the speed and determination of Russia's hybrid war against Ukraine, but they would not have been had they witnessed the extensive subversive effort Russia made in pre-war Ukraine. Russia's destabilisation of Ukraine eventually culminated in the invasion of Crimea. That direct action, with Russian deployment of 'little green men', retained the characteristic of deniability. That said, non-direct action remains the principal manifestation of hybrid threats – although its use by powerful players such as Russia contains within it the latent threat of potential follow-up violence.

Europe today: Fertile territory for hybrid threats

The EU today provides several opportunities that external adversaries can exploit. Three main factors matter: the changing post-cold war geopolitical environment; technological and legal vulnerabilities inherent in globalisation and the common market; and a post-historical zeitgeist still prevalent in Europe that does not accept that subversion, let alone direct military action, is a threat to the European way of life.

In the 1990s Europe was largely surrounded by reforming states or infant democracies preoccupied with their own transformation. Now, the continent neighbours ambitious powers that seek to project both hard and soft power in Europe. Many of them work with anti-system forces in Europe as well. This power projection can have a variety of aims, including that of spreading states' repressive instincts and ideologies to Europe, which may involve silencing, suppressing, or even eliminating dissidents residing there. Such states may also want to control the narrative on their domestic developments through information operations targeting emigrant communities, but also by gaining control of cultural and religious organisations. In Europe, Russia is the best-known actor in these respects, but Turkey and Iran are also active. Saudi Arabia's influence operations concentrate on the US, but some of them are visible in Europe.

Another development is the rise of China and the increasing assertiveness of its state apparatus. While Chinese influence operations are less visible than Russian ones, Chinese economic espionage is very active; China sees Europe as a softer target than the US. It concentrates on launching skilled cyber attacks against industries and research facilities, but its programme also encompasses strategic investments in key technology industries.

As these changes have taken place, the EU's digitalised economy and increasingly open and interconnected society have provided hostile foreign actors with a wide range of attack points. Digital infrastructure – from military communication to 5G transmitters, to voting machines – enables hostile actors to successfully access an increasing amount of data and intelligence. Attack points are increasing in number, with the coming of the internet of things – with Alexa speakers, WiFi-activated lights, and smart thermostats used by European ministers and Uber drivers alike. Non-state cyber criminals will make use of these vulnerabilities, but hostile states can also exploit them.

Europe's increased vulnerability to hybrid attacks is not a risk inherent in technological progress and globalisation: it is a matter of choice. Europe has settled on a laissez-faire approach to these issues. Both Europe's public and political elite alike have largely developed a Fukuyaman, end-of-history world view that does not measure up to the harsh global and regional reality Europe faces. The wars in Ukraine and Syria have made some small dents in this world view, but most Europeans remain fundamentally untroubled by the dangers swirling around them. Despite modest increases in recent years, European overall defence spending has only returned to 2008 levels.

All this is reflected in Europe's political culture, which remains one that very much seeks resolution through dialogue rather than confrontation. As a result, when confronted with geopolitical bullying – such as through hybrid threats or hyper-aggressive intelligence action – European governments' first instinct is that patient engagement will resolve issues. The option of a strong response is deeply uncomfortable for the public and politicians in most of the EU.

Fundamentally, the flipside of Europe's diversity and openness is that it retains a patchwork of approaches to hybrid threats. There are huge differences between the urgency, importance, and methods with which European countries combat these threats. For some states, and even

[1] Telephone interview, 7 February 2019.

political parties, taking these threats on is a full-time state activity; for others, 'hybrid threats' is a temporarily fashionable term peddled by geopolitical scaremongers. Thus, resources, competencies, and political choices focused on hybrid threats vary wildly across the EU.

The EU's role

Parts of the EU's machinery have been very active on these matters, but it still lacks a holistic approach to them. In recent years, new communications, laws, strategies, task forces, funding, and member state working groups have emerged to bolster the EU's security and resilience. For example, in 2017 the EU set up a Cyber Diplomacy Toolbox. The EU's cybersecurity agency, the European Union Agency for Network and Information Security (ENISA), is set to receive a revamped, and stronger, mandate. Speaking to ECFR, one senior European official dealing with cybersecurity characterised ENISA as "frankly, a think-tank".[2] Even with the revamp, it will remain a tiny agency by any standards: the number of staff it employs is set to rise from 84 to 125, and its budget is set to increase from €11m to €23m, over the next few years.

This process has been somewhat reactive and still lacks high-level political leadership. One senior member state diplomat has remarked that: "The EU Council and member states' response to hybrid threats in Brussels have been mostly driven by the Skripal affair. The Commission has been doing a lot of work on cyber and the security union. The [European External Action Service] has done plenty of good things on the working level – good action plans, task forces, conceptual work. But Mogherini does not want to touch the subject. And there is little sense of coordinated and strategic work on the matter. And many think [it is] just another irritant on the agenda of EU-Russia relations."[3]

Increasing adhocism accompanies this incremental institutional progress – which takes the form of coalitions of the willing cobbled together on a case-by-case basis, beyond the realm of EU bodies. These developments point to a lack of ambition for a more coordinated EU-level response. This is especially the case on the most threatening hybrid attacks. For instance, diplomatic expulsions over the Skripal affair took place outside the EU framework. And so did public attribution and indictments against Russian operatives who tried to hack into the Organisation for the Prohibition of Chemical Weapons (OPCW). When that incident became public, non-EU member states such as New Zealand, Australia, Canada, and the US released statements in support of the Netherlands that were more forceful than those from half a dozen EU member states. And this was despite the fact that the OPCW headquarters is located in EU territory. One senior EU official recounts excruciating meetings in which some member states stonewall others when they try to obtain support to attribute attacks to state-backed hacking groups This is despite reams of cyber forensic evidence and intelligence assessments.[4]

Some EU member states that acknowledge hybrid threats as a major priority have appointed special ambassadors or created dedicated units within the government or their foreign affairs ministries, to coordinate responses to these threats. Among them are Sweden, Finland, Poland, Lithuania, and Spain. This list suggests a particular concern with Russia. Spain is a geographic outlier but, as one European diplomat explains, the 2017 independence referendum in Catalonia forced Spain to rapidly prioritise hybrid threats.[5] The biggest EU countries, France and Germany, have not really internalised the notion of hybrid threats yet, but both have been seeking ways to respond to them. States such as Austria, Hungary, and Italy do not yet appear to be much concerned with hybrid threats.

Overall, despite increased EU and member state activity on cyber issues, a lack of coordination and leadership from the top means that hybrid attackers continue to have diverse opportunities to conduct operations. Some of the EU's external competitors are less than fearful of its efforts. Vladimir Putin's special representative on information security has compared Russia to a cyber elephant and the EU to a small, irrelevant barking dog. So, the question for Europe concerns how it can build up its capacity to resist hybrid attacks, while also adopting a foreign policy posture that is not simply defensive but actually contributes to a gradual reduction of the threats directed at it.

Intelligence agencies and hybrid threats

Intelligence activities are central to efforts to combat hybrid threats: intelligence agencies are usually the first to do everything from tracking cyber attacks to identifying foreign funding for violent anti-system forces. Other investigative forces, such as police and prosecution services, rely heavily on them. However, a multiplicity of actors is involved in intelligence: the military, the police, national intelligence services, national cybersecurity agencies, private companies (which also have cybersecurity obligations), media actors, NATO, the EU, Europol, and ENISA.

This institutional hotchpotch is mirrored by a wide variation in national bureaucratic security cultures. One official working on this subject outlines the challenge in the following way: "Hybrid threats come from outside the EU, but the way you combat it is through institutions that deal with domestic issues – police, media watchdogs, education systems, border guards, anti-corruption watchdogs."[6] However, it is not just, or even mostly, the proliferation of agencies and actors that had created the EU's inadequacies in this area. A lack of political leadership is also responsible. The same official adds that: "the [agencies] don't have the culture and often the desire to be combating external threats. Especially because some of these threats are certainly no good, but they are not illegal: fake news, conspiracy theories, trying to influence history narratives or manipulate identity issues and feed culture wars is not illegal. Quite the contrary. They often are part and parcel of domestic political practices." Aggressors take advantage of this legal patchwork by picking the jurisdictions with the weakest regulations as bases from which to conduct operations in other countries.

A basic lack of resources is also a major problem. There are few fields in which Europe as a whole is so dependent on American support, and where the discrepancies between the haves and have-nots within the EU are as great, as in intelligence. Today, only the United Kingdom and France have the requisite legal frameworks and capabilities to

[2] Interview with EU official, Brussels, 12 March 2019.

[3] Telephone interview with EU member state diplomat dealing with hybrid threats, 25 January 2019.

[4] Interview with EU official, Brussels, 12 March 2019.

[5] Telephone interview with an EU member state diplomat, 11 March 2019.

[6] Telephone interview with EU member state diplomat, 11 March 2019.

conduct intelligence and counter-intelligence operations in all spheres. And there are many strands to this:

- Strategic intelligence: predicting or anticipating the moves and interests of other countries' leaderships, as well as their decision-making preferences.

- Operational intelligence: detecting, identifying, and monitoring the enemy's operational assets (including diplomatic, economic, military, and paramilitary assets) and anticipating their moves, orders, operational priorities, and use of tactical means (such as troops, money, and propaganda).

- Signals intelligence: intercepting the enemy's communications before decrypting and analysing them to gain access and insight into its command-and-control processes.

- Electronic intelligence and corresponding intelligence on other emissions and signatures: collecting emission fingerprints (signatures) of enemy weapons systems, sensors, platforms, and communications systems to detect their deployment and activity, work out their capabilities, and find ways to intercept, decrypt, deceive, or defeat them.

- Counter-intelligence: detecting, monitoring, and foiling the enemy's attempts to gather intelligence on oneself in all the areas mentioned above.

After the end of the cold war, European armies refocused on expeditionary warfare and asymmetric threats. Most intelligence services went through a similar adaptation process. Hostile sub-state groups, terrorist networks and radicalised individuals – rather than hostile state actors – became intelligence services' main focus. While this was necessary, state actors have made a comeback in recent years.

Currently, most European intelligence agencies rely on human intelligence – people with personal knowledge of foreign decision-making processes – to tell them what is going on in other countries and anticipate the moves of these states. They do not have a chance to validate – or invalidate – this intelligence through other sources, particularly signals and electronic intelligence. This means that they do not know whether their intelligence is accurate and, therefore, whether they should act upon it. In addition, European intelligence efforts are often confined to operational intelligence in theatres close to Europe (such as north Africa and the Balkans), where European troops and foreign assistance programmes are at risk. Only a few European states are capable of systematically developing sources in countries such as China, Iran, Russia, Saudi Arabia, and Turkey to gain insight into what their governments and bureaucracies are up to. For most other states, strategic intelligence is little more than guesswork.

Yet even the EU's best-equipped intelligence services are not equal to those of the US or China. They still rely on cooperation with the US to safeguard their countries' interests. For some European countries, this dependence is particularly great. Indeed, the truth is that most European states would not be able to prevent terrorist attacks without intelligence provided by US agencies. Most European states have effectively outsourced intelligence to their US ally, enabling them to make out that they have not engaged in activity their citizens may dislike but nevertheless benefit from.

Current 'hybrid threat' policy challenges

Despite creating a series of strategies to combat hybrid threats, Europe's response to the issue is generally still in the thinking, rather than acting, phase. Several ongoing policy debates are illustrative of the divergence between European countries' views, and of the reluctance to decide how to deal with the regulatory and administrative consequences, of such threats. These debates include those on how to deal with Russian election interference, how to respond to Russian cyber attacks, and whether to use Kaspersky and Huawei products.

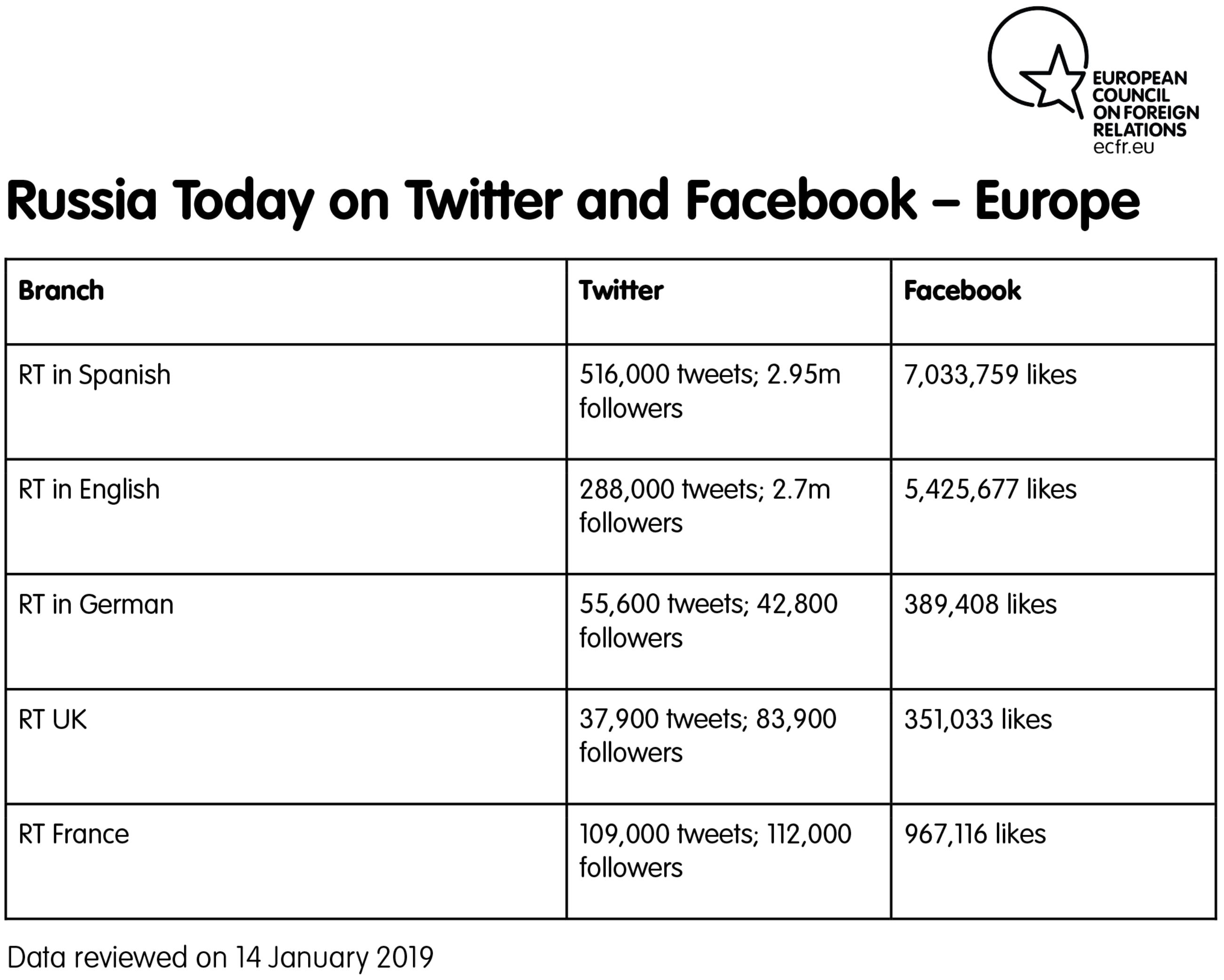
Russia and election interference

Europe lacks a unified understanding of the level and scale of Russian attempts to interfere in European electoral processes and referendums. Most Westerners assume that Russia has indeed tried to influence some elections. By now, most European and American citizens know much more about the exact scope, techniques, and even operators that tried to influence the 2016 American presidential election than about any Russian interference in European elections and referendums. In the US, the Mueller investigation has helped publicise evidence of the Russian effort to influence the presidential election. So far, 25 Russian citizens involved directly have been named. Their indictments give specific and credible details of names, procedures, and money flows. Even Russia seems to no longer dispute these activities. In this sense the US has made more progress than Europe has in understanding the exact nature and scope of Russia interference. This is despite the fact that, in all likelihood, the Dutch informed the US of Russian cyber intrusion into the presidential election early on.

In Europe, while there is much talk about Russian interference in European elections, a lack of proper investigation into these activities means there is also much scepticism about the reality and scale of such interference. Sections of the European public and political elites see Russian attempts to influence elections everywhere. Equally large sections of the public and political elites do not see them anywhere. The discussion on both sides is often speculative.

The activity of Russian state-backed news outlets such as RT suggests that bodies linked to the Russian government at least play a role in seeking to shape European domestic opinion. RT appears to support whatever destabilises European politics at any given moment: referendums in Scotland and Catalonia, *gilets jaunes* protests in France, and the activities of populist parties across the continent. This is all in plain sight.

In a recent analysis of 24 million Brexit-related tweets, cybersecurity company F-Secure concluded that there had been systematic, often automated, efforts to boost pro-Leave groups from abroad. Many pro-Brexit Twitter accounts have also been active in supporting the *gilets jaunes* protests in France. In countries such as Georgia, Poland, Romania, and Ukraine – each of which has a reasonably strong anti-Russian political consensus – Russian information operations have mostly focused on promoting anti-EU and



Russia Today on Twitter and Facebook – Europe

Branch	Twitter	Facebook
RT in Spanish	516,000 tweets; 2.95m followers	7,033,759 likes
RT in English	288,000 tweets; 2.7m followers	5,425,677 likes
RT in German	55,600 tweets; 42,800 followers	389,408 likes
RT UK	37,900 tweets; 83,900 followers	351,033 likes
RT France	109,000 tweets; 112,000 followers	967,116 likes

Data reviewed on 14 January 2019

anti-NATO sentiment and 'neutralism', or equidistance between Russia and the Western alliance.

However, it is unlikely that Russia is involved in every disinformation campaign that takes place in Europe. In some of these campaigns, Russian disinformation activities have been absent or modest, or have paled in comparison to local political parties' manipulation of the media. For instance, when Facebook took down 168 accounts trying to influence elections in Moldova, most of the accounts were local, not Russian. The Macedonian referendum held in September 2018 also attracted claims of Russian interference. But none of the multiple political players ECFR asked about this on a visit to Skopje during the campaign – from the prime minister to political party operatives and pollsters – had seen a massive Russian operation to sway the vote. And Donald Trump, Brexiteers, and the French far right have had much greater success than RT or Russian trolls at spreading fake news and conspiracy theories.

European countries' law enforcement agencies and parliaments have barely even begun any sort of systematic and detailed attempts to untangle myth from reality in Russian attempts to influence European elections and referendums. This allows intra-European mistrust to grow. Even states with similarly critical views of Russia do not entirely trust each other on this question, underlining the difficulties of forging a unified understanding of the threat. For example, one Nordic diplomat interviewed for this paper was convinced that the UK's Conservative Party had deliberately stonewalled a full investigation into the Russian role in Brexit because this would have been embarrassing for it – as the champion of Brexit. If they aim to devise policies that strengthen their sovereignty, European countries must gain a coherent shared understanding of the threat that Russian interference poses to their domestic politics.

Russian intelligence

Russia's interference in European elections has primarily been an issue of disinformation, igniting a controversial debate on media standards and political accountability of internet companies – Facebook and Twitter above all. But the issue of how to deal with Russian intelligence operatives is even more explosive for European cohesion. For example, after the Skripal attack, EU member states Austria, Cyprus, Greece, Hungary, Slovakia, and Slovenia did not expel Russian diplomats. This led to a discussion on solidarity among EU states such as the UK – having witnessed a Russian-sponsored chemical attack on its soil – wanted to send as strong a message as possible. The Austrian government's explanation of its reluctance to expel diplomats – that it should not take sides but serve as a "bridge" between east and west – further irritated other European governments, as it suggested an equivalence between an external aggressor and the EU member that had been targeted.

The activities of Russian intelligence services increasingly pop up in public security debates. In some cases, the known activities of Russian operatives involve classical espionage. In others, their activities hint at much more robust subversive aims: cultivation of anti-system forces, the purchase and preparation of infrastructure for future military incursions, training for paramilitary resistance groups, and the assassination of perceived enemies. These actions are top-tier covert actions. One may assume that other actions that provide the basis for this sort of activity – such as strategic reconnaissance, cyber penetration and espionage, excavation of data, the placement agents in positions of power, and reconnaissance of critical infrastructure – have progressed as well. Europe has a mixed record of disrupting these preparations.

While EU member states on the eastern flank have adopted very robust counter-intelligence laws and invested significant resources in monitoring Russian operatives, other states are more reluctant to do so. France has the legal framework for such action, but counter-terrorism is its first priority. Germany and Austria – both countries that were under Allied supervision and occupation after 1945 – have comparatively weak laws, and their decision-makers maintain a 'hands-off' mentality. In the past, bilateral cooperation with US services addressed these imbalances. As a legacy of the post-war situation, US and British services have the right to engage in counter-intelligence work in Germany. And Berlin, which has historical issues with counter-intelligence, has been happy to outsource this politically toxic work. In doing so, Washington – and to a lesser extent London – became an external balancer in intra-European affairs. And while the Trump administration and its sometimes erratic personnel have significantly undermined confidence in the US government, the US intelligence community has remained much more stable and able to preserve working contacts throughout Europe. But if relations with Washington deteriorate further, there is no tangible policy or political actor that could replace the US.

Kaspersky and Huawei

What should Europe's defence and foreign ministries, intelligence services, and telecommunications giants do about Kaspersky's anti-virus programmes and Huawei's telecommunications equipment? Are companies such as these a potential conduit for the collection of intelligence and data by foreign powers? Can they hold critical infrastructure in the EU hostage in the event of a major crisis between Europe and Russia, or Europe and China? These two companies currently find themselves in the eye of a political storm, but there are likely to be similar controversies involving other non-EU companies as well. These could include ZTE, Xiaomi, Lenovo, data centres around Lake Baikal, or even Uber-style taxi services such as Yandex Taxi.

The European Parliament has already singled out Kaspersky and called for a ban on malicious cyber products. The UK, Lithuania, and the Netherlands have followed the US in banning Kaspersky software from government agencies. Lithuanian officials have been advised against using Yandex Taxi, for fear it would transfer personal data, including location data, to Russian state structures. Others disagree, however: Belgium, Germany, and Interpol have given Kaspersky anti-virus programmes a clean bill of health.

Even within countries, approaches can differ. Several years ago, Kaspersky won a tender for the French ministry of defence. Now, the ministry is weaning itself off Kaspersky anti-virus products, gradually replacing them with anti-virus software from British and Japanese companies. At the same time, the head of the French National Cybersecurity Agency seems more sanguine about Kaspersky. In his view: "Kaspersky is clearly in the centre of a conflict pitching the Anglo-Saxon world against Russia."

Anti-virus programmes can at least be used under controlled conditions, or easily replaced in what is a competitive market. States disagree on whether Huawei equipment could be used to spy on or disrupt entire telecommunications sectors. Some, such as France, have been sceptical of Huawei for years, while others, such as the UK, have been more welcoming.

Huawei participation in the deployment of 5G mobile networks has become a political hot potato and a source of diplomatic tension and political rows between the US and some European countries, within governments such as those of Italy and the UK, and between private sector companies and governments. There are new twists in the Huawei story every week in Europe.

Another problem is that, even if EU institutions and some European governments were ready to engage in more forceful diplomacy with China over cyber espionage, many, if not most, affected companies and some other countries do not even want to talk about the problem, let alone act against it. This is due to fear of Chinese retaliation and a potential loss of access to China's markets.

The issue of European sovereignty in software and hardware is not confined to questions around Russia and China. For instance, take the case of Palantir, a US software company that is widely used by law enforcement agencies and intelligence services for big data analysis. French members of parliament have raised questions about Palantir. One asked the chief of the French cybersecurity agency the following question: "The software of Palantir, a company linked to the CIA, is used by the general directorate for internal security since 2016 to analyse billions of units of online data. Is it technically possible to disconnect from Palantir? Would it be possible to replace it?"

The agency director responded: "I confess I do not understand why we are not capable of creating a European Palantir. I think this is achievable. If we give up analysing data ourselves, we will be condemned to be data vassals."

As with the question around Russian interference in elections, the use of Kaspersky and Huawei, or even Palantir, demonstrates that Europe has not even begun to agree on what the problem is. Hundreds of technical experts have been looking into these companies' performance, and they have reached no consensus. And, were a significant number of EU member states to agree to prevent these companies from operating altogether, it would remain unclear how they should go about this. A failure to resolve these issues could put at risk cooperation and exchanges between intelligence services or military services if they did not trust each other's anti-virus software and telecommunications gear.

Cyber attacks

Cyber threats have increasingly moved beyond financial theft, cyber criminality, and intelligence collection into much

France and fake news

Fears of combined cyber and information attacks are driving some countries to patch up their electoral practices. Anti-fake news campaigns, laws, and other efforts are under way in several EU countries. France is a relevant case in point. "MacronLeaks" was an attempt to influence the French presidential election in 2017 by hacking and dumping information from Emmanuel Macron's campaign headquarters. This attack was attributed to Russia. The attempt largely failed not just to influence the campaign, but to even get traction in the media and the wider public. One key reason that it failed was because there was no well-oiled transmission belt connecting the darker corners of the internet, where the hacked information was posted, to the wider public. No major French media outlets reported details from the dump, and whoever wanted to spread disinformation had no network of French Twitter or Facebook followers through which to do so. Since 2017, France has adopted an anti-fake news approach, but the problem is now that the transmission belt for similar attacks in the future is in place in the form of the popular, and reasonably 'nativised', RT France, which launched in early 2018. Should an operation such as MacronLeaks be conducted in 2019, it would probably be more successful than the effort two years ago. In 2017 MacronLeaks was played on a tiny speaker for a tiny audience; in 2019 it would use a powerful surround-sound system of television, websites, and social media.

more aggressive actions designed to shape national debates, referendums, and elections in European countries. According to Europol, a growing share of these attacks are the work of state-supported hackers, rather than just criminal cyber syndicates or bored teenage hackers working from their bedrooms. And there continues to be a lack of preparedness for this on the part of EU and member state institutions. ENISA states that: "Should a crisis arise from a large-scale cyber incident, Member States would lack a harmonised framework to effectively respond to the challenges posed by this incident."

Cyber attacks have also taken a political turn, thereby demonstrating their hybrid potential. Unfriendly states have done this in several ways, from releasing hacked information to seeking to discredit and intimidate political actors, to using fake or automated accounts. Disinformation, rumours, and manipulation have always existed in politics, and have always been driven by both domestic and external players. Now, they can reach directly, through social media, into a much wider spectrum of society. This is especially the case because of the current political turbulence in Europe and the lack of agreed-upon, Europe-wide safeguards.

EU member states currently pursue one of what might be termed 'two and a half' approaches to countering these dangers.

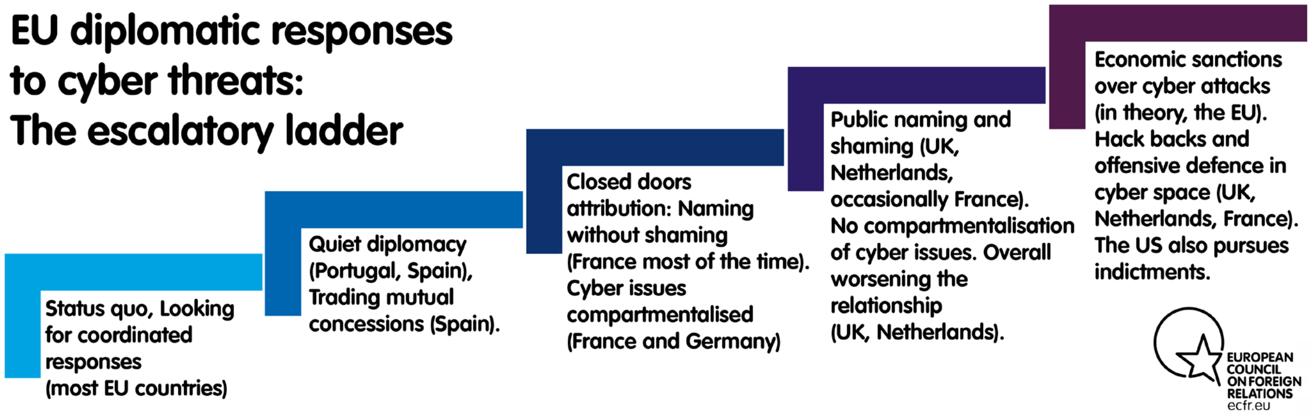
The 'half' approach involves maintaining the status quo. This has evolved from a laissez-faire response to soul-searching on what to do about hybrid threats. Most EU countries are still at this stage. Many have identified hybrid threats as a priority and, as mentioned above, some have appointed special ambassadors as a result. But these countries are still very much in the search phase on specific policy issues such as how to respond to cyber attacks and how to handle RT.

When the search phase draws to an end, it usually results in countries selecting one of two types of approach. One is to pursue a more or less formal 'cyber dialogues' with external powers, which could be official-to-official or minister-to-minister. Another is to start pushing back through public attribution, by 'naming and shaming', and even contemplating indictments, sanctions, or cyber counter-attacks (so-called "hack backs").

Options for the EU

Dialogue

Talking to those who launch hybrid operations is an option perfectly in tune with the European predilection for dialogue. The philosophy that guides this is that a good talk is always better than a good fight. And it is the right approach when it works. But it often does not work, such as in the US-China cyber dialogue initiated by Barack Obama in 2015, which resulted in an agreement to hack each other less and, seemingly, only a short-lived lull in aggressive cyber behaviour.



EU diplomatic responses to cyber threats: The escalatory ladder

Status quo, Looking for coordinated responses (most EU countries)

Quiet diplomacy (Portugal, Spain), Trading mutual concessions (Spain).

Closed doors attribution: Naming without shaming (France most of the time). Cyber issues compartmentalised (France and Germany)

Public naming and shaming (UK, Netherlands, occasionally France). No compartmentalisation of cyber issues. Overall worsening the relationship (UK, Netherlands).

Economic sanctions over cyber attacks (in theory, the EU). Hack backs and offensive defence in cyber space (UK, Netherlands, France). The US also pursues indictments.

Some states have taken this road. For instance, France has launched cyber dialogues with Russia. In late 2018 Spain and Portugal also launched their own bilateral cyber dialogues with Russia. Moscow has allegedly offered to conduct such a dialogue with London as well. The aim of these efforts is to persuade the originator of the hybrid threats to cease acting in a hostile manner, including by agreeing to an implicit code of conduct or even a non-aggression pact. Such dialogue could result in agreements not to hack each other's critical infrastructure or election infrastructure. Cyber dialogues have their limits, though: it is hard to believe they would ever cover hacking for cyber intelligence collection, given the sensitivity of this area.

For a country engaged in such a dialogue, what can it offer a state such as Russia? For those with more or less significant offensive cyber capabilities, such as France, an exchange of mutual favours in the cyber domain might be feasible – as was the case with the US-China agreement. But, because most EU member states have only meagre cyber capabilities, they are unable to offer many cyber concessions to trade with a country such as Russia. Thus, the mutual exchange of favours can only become meaningful if it includes mutual concessions from other policy domains, and not just cyber. Witness, for example, the following exchange between the Russian foreign minister and his Spanish counterpart in November 2018, a year after the Spanish foreign and defence ministries openly railed against hostile online activities designed to fuel the independence movement in Catalonia:

> *Sergey Lavrov: I spoke with the minister about this today. He said that some Russian media go beyond their journalistic mission and are involved in unacceptable interference in domestic electoral processes in other countries. I told the minister, as I am telling you now, that we prefer to discuss such issues professionally rather than with a microphone. We do not want our relations with Spain, our good friend, to go awry. I reminded my colleague that we have repeatedly suggested to our European and US partners establishing bilateral working mechanisms on cybersecurity issues. We stand for discussing emerging issues through dialogue. It seemed to me that our Spanish partners are interested in the idea of establishing a working group on cooperation in ensuring cybersecurity.*
>
> *Josep Borrell: We never said it was the government of Russia, but it is true that [the false news] came from Russian media.*

Borrell thanked Russia and Putin for indicating that they: "will always support the sovereignty and territorial integrity of Spain at a time when pro-independence groups have been trying to proclaim the independent republic of Catalonia." Three days after this exchange, the Spanish port of Ceuta, in north Africa, was reopened to Russian naval vessels on their way to Syria.

Such dialogues may form part of Russia's tactics to either block organised responses to its hostile operations or to drive wedges between European states. Russia has long sought to divide the EU on policy issues such as energy, visas, and foreign policy. Now, it applies the same approach to the cyber domain. Dialogues can thus serve the purpose of enabling endless, or at least excruciatingly long, rounds of cyber talks that do not force Russia to change its cyber behaviour. Alternatively, such dialogues can also lead to genuine cyber détentes for some EU member states, but not others, leaving plans for a pan-EU response or strategy in tatters. The launch of cyber dialogues with Spain and Portugal happened just around the time when tensions between Russia and the UK and the Netherlands reached a peak over the Skripal affair and Russian attempts to hack into the Hague-based Organisation for the Prohibition of Chemical Weapons.

Pushback

Where polite diplomacy fails, states have adopted more assertive ways to push back against hybrid and cyber threats. In these states' view, the laissez-faire approach to attribution and the lack of pushback against aggressive cyber tactics has turned the cyber field into a free-for-all for rapacious cyber entrepreneurs, one in which the costs of aggressive misbehaviour are virtually zero.[7]

France is an interesting case of a state that started a dialogue on cybersecurity issues with Russia in mid-2018, but has since publicly attributed several operations to Russia. One French diplomat told ECFR that: "aggressive public attribution with Russia will not work, and is not in the style of French-Russian relations. We tell them what we know with a firm voice, but behind closed doors."[8] But such patience is periodically punctuated by public attribution at the highest political level. Emmanuel Macron has accused RT of acting as a state-backed agent of influence, and the French defence minister has pointed to Russian state-supported hacker group Turla as being a major and constant source of cyber attacks against the defence ministry.

A key reason to publicly attribute attacks is not just to persuade foreign actors to back down, but also to shore up support for government action among the wider public and allied countries. In this, attribution is also an exercise in building greater resilience: preparing and educating the public and parliamentarians about what has really happened, drawing attention to the matter, and building support for possible diplomatic or sanctions responses. In the Skripal case, the UK responded with a vigorous campaign that laid the blame firmly at Russia's door and that involved sharing intelligence with partners across Europe. Such tactics met the goal of ensuring the UK did not stand alone in a major international incident, at a time when its relations with the rest of Europe were strained over Brexit.

Furthermore, by adopting an aggressive name-and-shame approach, the UK forced Russia into a defensive mode in which it made several mistakes that all but confirmed its involvement. When the UK accused two alleged Russian intelligence officers of the poisoning, the two individuals went on Russian television to deny their involvement. But they did so with such ineptitude and lack of plausibility that the British version of events suddenly looked much more persuasive – even to the staunchest doubters. This then sparked a search for the real aliases of the two Russian operatives, leading to the exposure of a whole network of Russian operatives – up to 305 – by Bellingcat, a network of citizen activists who cross-referenced a car registration

[7] Member state diplomat, remarks at ECFR EU-Russia Strategy Group, Madrid, 22 March 2019, under the Chatham House rule.

[8] Interview with French foreign ministry official, November 2018.

The pitfalls of attribution

Attribution of attacks in the cyber domain is notoriously difficult, though not impossible. Several high-profile cases have helped reduce public trust in professions of certainty based on intelligence, such as that preceding the military intervention in Iraq on the grounds that it had weapons of mass destruction. Attribution can rely on cyber forensics, but it has often relied more on intelligence sources, which can be harder to deploy publicly to change opinion and win wider support. Providing more detail may help adversaries close their security loopholes. For example, just three weeks after US intelligence services issued a report on Russian cyber activities around the 2016 presidential election, the Russian intelligence services arrested one head of department and his deputy from the FSB Cyber Centre for Information Security for being CIA moles. In such circumstances, Western intelligence services are often reluctant to engage in public attribution that can devalue or endanger their sources.

Private companies can also be reluctant to publicly attribute cyber attacks to foreign states. It was not always this way: companies used to be happy to blame cyber attacks on foreign state-backed actors as they looked less inept if their cyber defences had failed in the face of supposed Russian or Chinese state-backed hackers rather than criminal cyber groups or teenage amateurs. But this is changing. Insurance companies now hold that a hack supported by a foreign state is cyber warfare and, therefore, refuse to provide compensation. This happened in the fallout from NotPetya, the world's costliest virus attack, which started in Ukraine but then affected dozens of companies around the world. The UK government accused Russia of attacking Ukraine's digital infrastructure with NotPetya. But when the virus spread and one of the affected companies – the maker of Cadbury chocolate – made an insurance claim for the attacks, its Swiss insurer refused to provide compensation, invoking the UK government's attribution of the attack to Russia as proof that NotPetya was an act of cyber warfare not covered by its insurance.

plate with a GRU address. So what started as a name-and-shame exercise by the UK ended up in a major diplomatic and intelligence debacle for Russia. Attribution also helped unify the European response, which resulted in the more or less simultaneous expulsion of Russian diplomats by 19 EU member states, and ten non-EU states.

Beyond naming and shaming, states have started to make greater use of indictments, counter-offensive cyber strategies, and even hack backs. Their goal is to change the calculations of foreign state-backed cyber actors by starting to impose costs – on the cyber actors themselves and the states supporting them. The US pioneered this approach, which has been increasingly adopted by the UK, the Netherlands, and, on a smaller scale, France. All three countries have changed their cyber doctrines to move from an almost exclusive focus on cyber defence and cyber intelligence collection towards the possibility of counter-offensive cyber actions. What drives this greater assertiveness is an understanding that toothless cyber diplomacy is not enough to combat the state-sponsored cyber threats to Europe.

Conclusion and recommendations

Dealing with hybrid threats involves action on several fronts. The first is the political front. The second is the digital home front. The third is the intelligence front: setting new goals and standards for intelligence services, and improving the coordinated approach within Europe. And, finally, EU member states and the EU itself can take steps on the diplomatic front to deal with foreign powers that conduct hybrid operations against them.

The political front

The European conversation on hybrid threats is polarised between political actors that see Russian interference in every European election and those that are completely dismissive of such fears. Europe would benefit if accusations of foreign interference were better supported with facts and details – such as those the Mueller inquiry provided in the US. Despite a plethora of journalistic investigations, and periodic statements from politicians, European legislative and judicial bodies have released few details about their assessment of the situation. This certainly does not help the EU arrive at a more united understanding of the scope of threats it faces.

Key instruments for creating a more unified awareness across Europe lie in the hands of national elites. These include more systematic use of parliamentary or UK-style public inquiries (such as the Chilcot and Leveson inquiries) and more systematic law enforcement work to pursue those who broke electoral law by attempting to influence votes through digital or financial activities.

The digital home front

On issues such as election interference, one way to hedge against the vagaries of the digital age is to return to analogue methods. The Netherlands reverted to paper ballots and hand counting in elections in 2017 as insurance against cyber tampering with voting machines and digital infrastructure. On some occasions, internet giants have chosen not to run political adverts at all – Facebook took this course during the recent Nigerian election. And, after Canada introduced strict requirements on the transparency of electoral adverts, Google decided not to run these. This is not a long-term solution, but it could be a temporary one until governments and these companies flesh out transparency rules governing campaign ads.

Dealing with cyber threats presupposes investment in the EU's capacities to deal with such issues. This requires several types of action:

- Transform ENISA into a well-staffed and well-financed cybersecurity institution in which multiple functions are centralised: computer emergency response teams (CERTs), cyber forensic teams, and legislative teams that drive up cyber hygiene standards across the EU.

- Within or outside ENISA, it is in the EU's interest to acquire a sovereign, pan-European capacity to investigate the sources of major cyber attacks directed at sensitive state institutions or critical infrastructure. This means beefing up European capacities for both cyber forensics, but also focusing and pooling together intelligence collection on cyber issues. Six EU member states have been leading the EU effort to build an EU Cyber Rapid Response Force that would help member states tackle serious cyber attacks. But once a crisis has been resolved, the EU also needs the capacity to conduct systematic, sophisticated, and post-factum analysis of the potential sources of cyber attacks. This would improve future protection and create the basis for subsequent diplomatic responses against suspected perpetrators (see below).

- EU member states should jointly invest in offensive cyber capabilities within PESCO. Lead nations such as France or the UK (if it stays affiliated with EU defence cooperation after Brexit) could provide the core capabilities that other states can build on. This would also avoid duplication of basic capabilities in every national cyber agency at the expense of more sophisticated cyber weapons, which can only be jointly developed. This is highly controversial for most EU member states. But key European states – and global or regional powers such as the US, Russia, China, and Israel – are already employing sophisticated cyber weapons. Even states that are sceptical of the ethical legitimacy of this will be affected by the employment of offensive cyber weapons by third states. And, sooner or later, they will want to benefit from the deterrent effect of European cyber weapons (and the threat to use them). Still, it remains to be seen whether such policies can be developed with all European states on board or whether it will be left to the most capable EU member states to spearhead the process.

- All European countries should improve personal cyber hygiene standards, both among the general public and in government. For example, European delegations consisting of diplomats from different member states behave in different ways when visiting state institutions in foreign countries that are perceived as aggressive in cyber space and electronic intelligence collections. Some European foreign ministries make their diplomats keep their mobile phones in Faraday cage bags when entering public buildings, while others do not. Indeed, many diplomats do not know what Faraday cages are. So, even a strong push to coordinate and spread core cyber hygiene standards for European diplomats, militaries, parliamentarians, and other officials would already constitute a step forward. The undertaking could include policies on: Faraday cages for European delegations travelling abroad; bans on the use of manufacturers' passwords in the public sector; and compulsory use of minimally safe passwords (checked against databases of compromised or leaked passwords).

The intelligence front

A European Investigative Service and a general prosecutor that works independently from member states would be best suited to tackling interference in domestic affairs and the subversion of state institutions by foreign intelligence services, as this would cut short attempts to suppress investigations for political reasons. That said, there is little chance that the EU will do this.

Any new European capacity would have to come on top of existing national capacities, to amplify and reinforce them. This will not make up for intelligence cooperation with the US in the short or even medium term. But it would certainly enhance European capabilities. The EU and its member states should consider the following actions:

- **Expand Europol's remit to include counter-intelligence**: Europol has long supported European countries' fight against organised crime, money laundering, and other transnational criminal activities. It has come across foreign intelligence operations in the past, some of which intersect with organised crime. Europol members should now create counter-intelligence bureaus, analytical cells, and data exchange formats to tackle cross-border activities. This would be particularly beneficial for small states fighting against foreign intelligence services' activities.

- **Set common legal standards on subversion and hostile intelligence services**: the legality of some intelligence activities varies between European countries. Counter-intelligence will not work without clear, legally binding definitions of what constitutes espionage, subversion, conspiracy, and hostile influence operations. Common standards would also facilitate cross-border cooperation between authorities, particularly in the indictment of suspects.

- **Tighten standards for financial supervision and investment screening of foreign state-affiliated actors**: Like organised crime, foreign intelligence operations require logistical infrastructure such as illegal residences; anonymous bank accounts or opaque financial schemes to funnel money to sources; fake companies and information networks; and fake news outlets to use for agitation. Greater transparency on real estate and corporate ownership would facilitate the fight against organised crime as well.

- **Establish a centre of excellence on subversion and counter-intelligence**: The NATO Cooperative Cyber Defence Centre of Excellence does a good job of analysing threats and compiling national situation reports. The constant exchange of information between various branches of government has increased member state bureaucracies' knowledge and understanding of this matter. The same approach would be helpful for counter-intelligence.

- **Introduce common procurement of strategic intelligence, surveillance, and reconnaissance platforms**: On hybrid threats, domestic counter-intelligence is often the focus of policy discussions. But in an escalating confrontation, the capacity to predict adversaries' military moves is pivotal. Europe needs to acquire airborne and shipborne strategic intelligence platforms. It currently lacks electronic- and signals-intelligence aircraft with long endurance and corresponding ground-based surveillance stations, particularly in the Black Sea. It also lacks stealthy autonomous aerial vehicles to collect intelligence in highly contested airspaces, such as Syria or Crimea.

The diplomatic front

European cyber diplomacy needs to become much more ambitious in developing a strong diplomatic infrastructure that reduces hybrid, cyber, and intelligence risks to the EU. It needs to do so jointly with potential allies. This infrastructure would need three layers: working with existing allies, fostering new cyber alliances, and developing assertive dialogues with states that are testing EU countries' defences with their hybrid tools.

Working with allies

The EU will never be entirely sovereign in the defence sphere without a nuclear deterrent. But there is no prospect of this unless France extends its nuclear protection to the entire EU and all other EU states accept it.

Even in other spheres, Europe is a long way from establishing a self-sufficient capacity to push back against hybrid, cyber, and intelligence threats. And even if it attains self-sufficiency, the EU's sovereign action will only become stronger if it can sustain strong allied responses to these risks coordinated with the post-Brexit UK, the US, Canada, and NATO. So, whether the EU has its own capacities to combat such threats or not, the first port of call will still be its closest allies in NATO – where a clear division of labour, or joint action with NATO, is likely to be the rule of thumb.

For NATO, the first task is deterrence (including nuclear deterrence) and defence. On hybrid threats, the picture is less clear. Hybrid operations are often a prelude to more intense pressure or even aggression. They are intended to erode the opponent's will or capacity to resist. The EU will remain the prime legal arbiter countering most hybrid threats to Europe. This is due to the EU's common space on security and justice, the close cooperation between its member states on homeland affairs, and the EU's legal authority over the common market (which is important on energy issues, fighting financial crime and illegal financial transactions, and border security) and its evolving competences in the digital space.

However, the EU should aim to closely coordinate its own procedures and policies with those of NATO. While Turkey blocks formal EU-NATO coordination, it is possible to circumvent this: EU member states can push for the same agenda and programmes within both organisations. This is particularly the case in planning and exercises for: NATO troops reinforcing local police detachments in frontline states in response to hybrid threats; NATO support capabilities (such as air transport, cyber troops, engineers); and emergency situations in Europe.

Finally, military and civilian intelligence sharing within NATO is important to Europe's overall preparedness for all sorts of threats – ranging from hybrid threats to traditional military threats. Exchange of experts and officials between Europe's inward-looking institutions (such as Europol and the European commissioner for justice and home affairs) and NATO's outward-looking assets and experts could improve their situation awareness. Here, too, member states need to circumvent the diplomatic impasse between Turkey and Cyprus by creating exchange forums on their own initiative.

Fostering new cyber alliances

The EU should expand its partnerships to combat hybrid and cyber threats in conjunction with friendly governments – in countries ranging from those in the western Balkans to Ukraine and New Zealand.

Friendly cyber partnerships can have multiple aims: capacity-building; providing assistance in establishing national cybersecurity strategies; addressing cyber crime; instituting cybersecurity standards; protecting critical infrastructure; and helping defend electoral processes from interference.

To a degree, the EU should conduct lawfare against its cyber adversaries. It is in EU's interest to become one of the driving forces of a global alliance promoting a crackdown on aggressive state-sponsored cyber behaviour through legal means. State-to-state dispute resolution is always difficult, not least in the cyber domain. Various models have been discussed in this respect. Some legal scholars have argued that state-sponsored cyber attacks fall well within the jurisdictional scope of the International Court of Justice, as they constitute potential violations of state sovereignty. Another form of legal and institutional pushback is to seek to create a World Trade Organisation-style dispute settlement mechanism for inter-state cyber affairs, in which an international body would have investigatory and adjudicatory powers. The EU should forge a global alliance of states that push for more assertive legal mechanisms to combat cyber threats through international law and international legal bodies.

Hard cyber talks

European efforts to forge global cyber partnerships should be matched by cyber dialogues with problematic cyber players such as Russia, China, North Korea, and Iran. One dictum of conflict resolution is that peace deals arise during mutually painful stalemates.[9] In the cyber domain, there is currently no stalemate: the situation is painful only for EU states. The nuclear détente in the 1970s was possible because each side was armed to the teeth and competition between them was costly. So, both had an incentive to slow things down. Today, most of the EU is a punch bag for hybrid and cyber operations.

Europe should pursue a 'dual track' approach of confrontation followed by dialogue with unfriendly cyber

[9] Jonathan Powell, *Talking to Terrorists: How to End Armed Conflicts*, Vintage, London, 2015.

powers. EU member states are currently split – some prefer dialogue on cyber and hybrid issues, while others have started to opt for confrontation because dialogue seems to be failing. To be more efficient, and to keep the EU united, Europeans will need to combine both approaches. Europe should actively work towards a series of cyber détentes by starting to be more confrontational about hostile behaviour directed at it.

A more adversarial dialogue will involve attribution behind closed doors, as well as periodic public attribution and even indictments of attackers if things do not improve. Hard-nosed trading of mutual concessions would supplement this approach. It could include mutually agreed red lines for cyber attacks: penalising attacks on critical infrastructure, including electoral infrastructure, but also tacitly accepting that some forms of hostile cyber activities will probably continue.

One can also look to gain leverage over the cyber field by conditioning free trade, investment screening, and development assistance on 'polite enough' cyber behaviour. Cooperation on combating cyber threats should become part of major EU partnership agreements.

***

Ultimately, to become more capable of dealing with hybrid threats on its own – to become more sovereign – the EU will have to start acting more like the US. This will involve investigating hybrid activities directed against European countries in much greater detail, and transparency about the findings of these investigations. European countries also need to move more quickly from the 'soul-searching' and assessment stage to fully acknowledgement of the scale of the problem and the adoption of a more robust form of engagement. This will involve a combination of dialogue with friends and adversaries alike, and engaging pushback such as public attribution. Without these measures, it is unlikely that Europe will attain any true degree of sovereignty in a world in which countries are increasingly liable to incorporate hybrid threats into their armouries.

Acknowledgements

The author would like to thank the officials who have shared their thoughts and analysis, including those from the Czech Republic, Estonia, France, Germany, Latvia, Lithuania, the Netherlands, Poland, Spain, Sweden, the United Kingdom, the European Commission, and the European External Action Service. Due to the sensitive nature of the topic, all of these officials prefer to remain anonymous. Thanks also go to Sven Herpig, Manuel Lafont Rapnouil, Tara Varma, Sico van der Meer, Thomas Reinholdt, and the participants in an ECFR brainstorming session on cyber diplomacy held in Madrid in March 2019 for their feedback on the ideas expressed in the paper or on the paper itself. The author would like to thank Marta Pellón Brussosa for her assistance in conducting research for this paper. Responsibility for the paper rests solely with its author.

About the author

Gustav Gressel is a senior policy fellow with the Wider Europe Programme at the European Council on Foreign Relations' Berlin office. His topics of focus include Russia, eastern Europe, and defence policy. Before joining ECFR, Gressel worked as a desk officer for international security policy and strategy in the Bureau for Security Policy of the Austrian Ministry of Defence from 2006 to 2014, and as a research fellow of the Commissioner for Strategic Studies with the Austrian Ministry of Defence from 2003 to 2006. He was also a research fellow with the International Institute for Liberal Politics in Vienna. Before beginning his academic career, he served in the Austrian Armed Forces for five years.

ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy.

ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Lykke Friis, and Norbert Röttgen.

- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia and Warsaw. Our offices are platforms for research, debate, advocacy and communications.

- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and "friends of ECFR" gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions.

www.ecfr.eu

The European Council on Foreign Relations does not take collective positions. This paper, like all publications of the European Council on Foreign Relations, represents only the views of its authors.

ISBN: 978-1-911544-89-0

Published by the European Council
on Foreign Relations (ECFR),
Berlin, London, Madrid, Paris, Rome, Sofia, Warsaw