THE NEW EUROPEAN SECURITY INITIATIVE

Edited by Ulrike Esther Franke,
Manuel Lafont Rapnouil
& Susi Dennison

EUROPEAN
COUNCIL
ON FOREIGN
RELATIONS
ecfr.eu

THE NEW EUROPEAN SECURITY INITIATIVE

Edited by Ulrike Esther Franke,
Manuel Lafont Rapnouil
& Susi Dennison

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.

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: 978-1-911544-22-7

Published by the European Council
on Foreign Relations (ECFR),
7th Floor, Kings Buildings,
16 Smith Square, London,
SW1p 3HQ, United Kingdom

london@ecfr.eu

Contents

Manuel Lafont Rapnouil

Introduction: Rethinking European security

If ever a reminder were needed, a succession of recent crises – Ukraine, refugees, terrorism – has demonstrated that Europe cannot hope to stand apart from global security challenges. And looking at what is already coming our way, this belated realisation will only be reinforced by cyber threats, tensions in the Pacific, or polarisation in the Middle East and North Africa.

At the European Council on Foreign Relations, we believe that Europe will be better off as an effective security actor on the global stage, rather than as the geopolitical plaything of others. This is why, since our foundation ten years ago, we have been working extensively on security-related topics. As early as 2008, Nick Witney's proposals for "Re-energising Europe's Security and Defence Policy" included a pioneer-group model for Permanent Structured Cooperation.

Since then, we have covered a lot of ground: from Mark Galeotti's influential work on Russia's intelligence services, coercive diplomacy, and criminal networks; to Ellie Geranmayeh's timely analyses and proposals at various moments of the Iran nuclear deal; to François Godement's recent work on China's view of the global order, at a time when Beijing's leadership is sometimes cast as the successor of Washington's.

But what we are faced with now is not just a continuation of the same old challenges Europe has always faced. Those challenges have evolved, and expanded too, from old conflicts to new threats; from the classical question of our relations with major powers such as Russia and China to the new face of the transatlantic partnership and the consequences of Brexit. From an international environment where we thought we could project stability into our neighbourhood, we have moved to a situation where the interdependence at the heart of the liberal order is being weaponised at our expense.

But, in the face of these challenges, there is also a new impetus to take them on. Policymakers' attitudes are beginning to change. Influential member states are changing as well. While Germany is showing a growing willingness to take on more responsibility, France is coming to terms with the inescapable need for more European military solidarity. Beyond these, other partners are participating in military overseas operations against terrorist groups. And discussions on flexible forms of defence and security cooperation will hopefully allow all European Union member states to contribute, and to cooperate with some of its closest partners such as post-Brexit United Kingdom.

ECFR's New European Security Initiative – NESI – has been created to tackle the questions that emerge at the meeting point of these two trends.

NESI will work on all four levels of European security: the threats, the capabilities that are needed, the coalitions and institutions that should deliver security, and the internal dimension of security cooperation within Europe. Our goal with this new ECFR initiative is to build on the cutting-edge expertise from all of our programmes and national offices to share in-depth analysis and innovative recommendations. Our work will rest on a firm military analysis, the deep wealth of our regional expertise, and our understanding of newer dangers of connectivity and emerging technologies. In true ECFR fashion, it will be grounded in the domestic politics of European states as well as in the complex decision-making of the EU. And it will break out of the compartmentalised frameworks of the past.

But this new impetus raises many questions. What are the threats that Europe faces? How does Europeans' understanding of security need to change? What precisely do we mean when we insist that the nexus between internal and external security needs to be addressed? How can we embed the traditional ideas of European defence efforts into a broader and more comprehensive understanding of what Europe's security, and Europe's contribution to global security, imply? What capabilities and equipment does Europe need to tackle future challenges? What forms of flexible cooperation, within and outside the EU, can we build that would help tackle current threats and challenges without undermining the EU's cohesion and solidarity? These are some of the questions that NESI will tackle head on.

Mark Leonard

The era of Mutually Assured Disruption

As the liberal order frays and geopolitical competition returns, it is natural that people turn to Henry Kissinger. No one has a more finely-grained understanding of power politics, and his treatise on world order sits on the bedside tables of many global leaders (even if few have actually read it).
But Kissinger's ideas of order represent an impossible aspiration in the world of ISIS and fake news. They are designed for a slower world of powerful states, rather than our age of permanent uncertainty, rapid change, and disruption.

Many traditional concepts – even well-tested ones – have been overtaken by events. Deterrence, alliances, even diplomacy, seem out of fashion; old certainties are gone. Kissinger's order was based on two pillars: legitimacy and balance of power. The defining moment of his worldview was the Peace of Westphalia. He laments the disappearance of the split between domestic and foreign policy. But, in spite of the return of power politics, the world is not 'Kissingerian' anymore.

Ironically, the person best placed to explain the new world died in early January this year: Zygmunt Bauman. Few people did more to help us make sense of the world we live in today than the Polish-British sociologist who developed the concept of liquid modernity. In Bauman's liquid modernity, many previously solid things have become fluid – jobs, sexual orientation, relationships, places of residence. Society is no longer held together by a collective project that offers the individual a sense of cohesion and direction.

Bauman was mostly interested in the liquid modern man and the individual's role in society. But the modern man has also given shape to a world in which security is defined by liquidity rather than order. Five forces are leading to 'liquid security':

1. Distinctions between foreign and domestic policy are no longer valid. Challenges like terrorism, cyber warfare, climate change, and refugee flows have removed the distinction between the internal and external, between domestic and foreign. This also changes our ideas of legitimacy, as foreign policy is no longer a prerogative of the

state but a central realm of domestic politics – one which is ripe for manipulation by outside powers.

2. There is no longer a clear divide between war and peace. It is many years since countries last formally declared war on each other. In the physical realm, many are trying out new kinds of coercion that fall short of conventional warfare – through little green men, coastguards impinging on international waters, or proxy wars through rebel groups. This is supplemented by a perpetual conflict between countries online that spans hacking and leaking to the destruction of nuclear facilities. The era of mutually assured destruction has given way to one of mutually assured disruption.

3. What brought the world together is tearing it apart. Connectivity – the idea that trade partners do not wage war against countries they have supply chains in – was heralded as the way to peace among nations. But now it is being weaponised. Dispersed networks used to be a safeguard against volatility, and international links a way to ensure good relations, if not cooperation, with everyone. Today, whether it is with sanctions or migration flows, countries are like spiders caught in their own webs, constantly threatened by enemies that are cutting away at the ends.

4. The time of firm security alliances is over. NATO has been declared obsolete by the American president, a statement that follows years of debates about the institution's usefulness. The European Union is losing a member and is weakened by internal disputes. In the age of Donald Trump and Recep Tayyip Erdogan, alliances will need to be built in different ways around domestic politics on every single issue rather than being taken for granted because of treaties and institutions. But, unlike the coalitions of the willing we have already seen in the past, they will rely much less on values and far more on narrow and short-term interests.

5. The world is no longer mainly defined by great power balances. A teenager in her bedroom can bring down companies and plunge societies into chaos by hacking into their systems. Whistleblowers and leaks pose disproportionate risks. A terrorist group can draw a state into open-ended wars. A tech company can determine what people see and thus what they believe. A reality TV star can entice the electorate and end up commanding the most powerful armed forces in the world. Players that

> we do not know yet may soon be deciding the fate of nations.

In Kissinger's old framework, legitimacy was defined by great powers. Today's legitimacy stems from deliberation and national politics, so we need to find ways of knitting alliances together by framing issues in ways that appeal to citizens in this new environment.

The ideal of international order has become an impossible aspiration. But flexibility, speed, and resilience will not be enough to live in a disorderly world without risking Armageddon. As frightening as Mutually Assured Destruction was during the cold war, it helped to take a particularly deadly option off the table. In today's world, we need to develop norms around the internet, economic warfare, and new technologies – if not to achieve order, then at least to create some boundaries to chaos that can save the world from implosion.

For the EU specifically, new mechanisms of collaboration and alliances are needed. In this dangerous world 500 million Europeans can no longer rely for their security on 300 million Americans. They will need both to invest in their security – and to transform their thinking. The EU needs to break out of the compartmentalised frameworks of the past, in which criminal, terrorist, economic, and military threats are viewed as separate challenges to be dealt with by separate and often competing agencies, each drawing on separate expertise.

The rationale for EU action must be grounded in the diverse domestic politics of its key member states rather than in the complex decision-making machinery in Brussels. EU institutions must find ways of empowering and bolstering member states and their ministers and governments. And new, more flexible arrangements are necessary to engage with post-Brexit Britain, with Turkey, Norway, and other neighbours. To make its citizens feel more in control in an era of uncertainty, the EU needs to liquefy rather than seeking impossible ideals of order. To hold this delicate balance will be the task of today's statesmen and stateswomen.

If security has become liquid, Europe's response must become more fluid as well. Traditional military analysis must be supplemented with an understanding of the domestic context of policing, anti-corruption efforts, intelligence, cyber defence, and sanctions. It must have a deep wealth of regional expertise, but have a wide enough lens to incorporate the newer dangers of connectivity and new technologies. It must understand the business models of the private sector actors that control the connections of the global economy. This is the guiding principle of ECFR's New European Security Initiative.

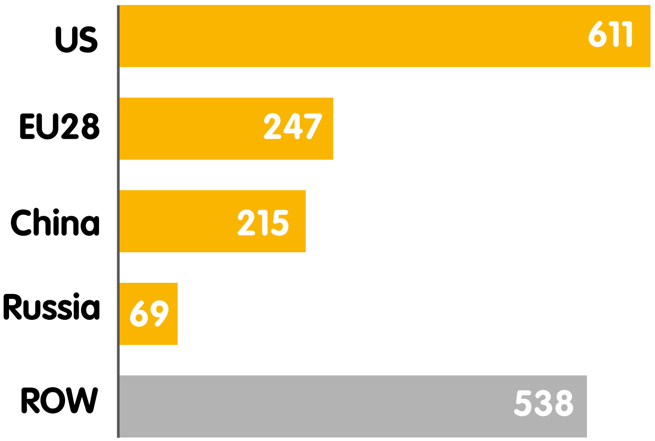
Nick Witney

Now or never on European defence

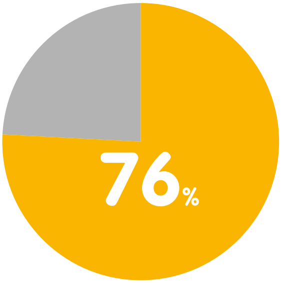
The unholy trinity of Vladimir Putin, Donald Trump, and the Islamic State group have caused defence to return to the top of the European agenda. And the conjunction of Brexit, Emmanuel Macron, and economic recovery has opened real possibilities for progress. The idea of a 'pioneer group' of member states, ready to move further and faster than others in deepening their defence cooperation, has been on the table for a decade – it is now time for the Franco-German couple to make it happen.

In the jargon (indeed, in the Lisbon treaty), this is called 'permanent structured cooperation' – PESCO for short. The idea is that an elite group shows the way in combining their defence efforts and resources to get more bang for their euro. This is a rather different focus from NATO's and Donald Trump's priority, which is to increase defence spending (the famous 2 percent of GDP target). It is also actually a more relevant one. The problem with European defence is less the overall quantum of money spent than the wholly inadequate output in terms of useful defence capability that Europeans get from the money they put in.

Global defence spending for 2016 ($US billion)

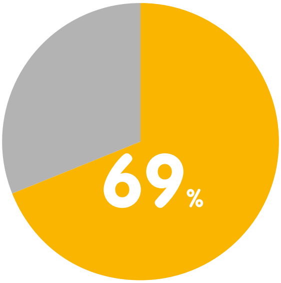


The EU 'big 5' make up



of total EU
defence spending

The 'Versailles 4' make up



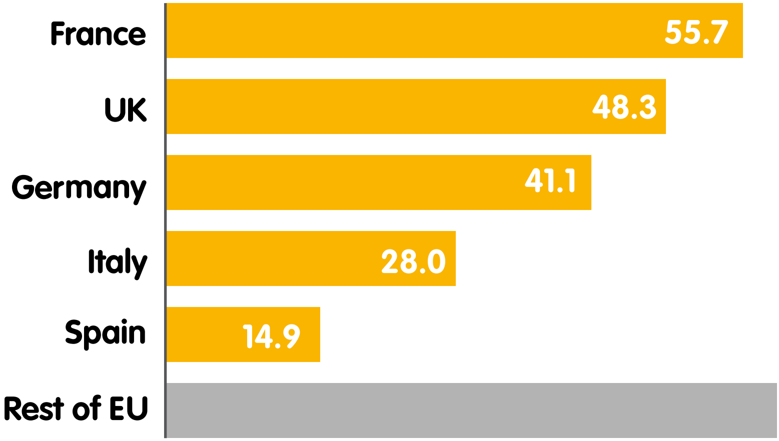
of total EU
defence spending

The combined defence expenditure of the EU28 is dwarfed by that of the United States. But, since even with Trump in the White House no one is yet envisaging war with the US, this comparison is irrelevant. More interesting is the fact that European defence spending still comfortably exceeds China's – and is an astonishing three and a half times bigger than Russia's. The fact that Europeans feel intimidated by Moscow's military power is testament to the appalling inefficiency with which they deploy their defence resources.

Of course, the idea that Europeans should integrate their defence efforts and cooperate more closely has been around for decades, and has even achieved some modest successes, on a project-by-project basis. But the goal of PESCO is to try to move this cooperation from the retail to the wholesale level. The pioneers are to make "binding commitments to one another".[1] The resistance and inertia in national defence machines will remain a big problem. But greater political pressure will have been mobilised to overcome this braking effect. And, since the treaty authorises the pioneers to self-select, the relatively small number of member states who are serious about defence can aim to press ahead without the further drag of a lot of unwanted hangers-on.

[1] Article 42 (6), Treaty on European Union, 2008, available at http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-5-general-provisions-on-the-unions-external-action-and-specific-provisions/chapter-2-specific-provisions-on-the-common-foreign-and-security-policy/section-2-provisions-on-the-common-security-and-defence-policy/129-article-42.html.

EU defence spending for 2016 ($US billion)



Not, of course, that anyone in Brussels can put things quite that way. There is understandably a great deal of sensitivity about the 'exclusive' nature of the PESCO concept, and an instinct to make it as 'inclusive' as possible. Back in the early years of this century, when the idea first emerged, many felt that it would be worth sacrificing a bit of efficiency in order to embrace as many member states as possible, especially at a time when the European Union was doubling in size. Binding new member states into PESCO would be part of the wider process of integrating them into the EU – and, little though they might have to offer, they were all such enthusiastic pupils. (My own attempt from those days to square the inclusive/exclusive circle may still have some relevance).[2]

But times have moved on. Europe's security environment has deteriorated, while a further ten years have been wasted with little to show for it beyond the further erosion of Europe's defence technological and industrial base. The sheer mechanical difficulty of getting anything meaningfully discussed and agreed 'at 28' has been repeatedly demonstrated. And, naturally, some of those enthusiastic new pupils have learned to misbehave. The old assumption that members of the EU must naturally share the same values and an instinct of mutual solidarity has taken a beating. No wonder there is now so much interest in the idea of 'multi-speed' Europe – with defence

[2] Nick Witney, "Re-energising Europe's Security and Defence Policy", European Council on Foreign Relations, 29 July, 2008, available at http://www.ecfr.eu/publications/summary/re_energising_europes_security_and_defence_policy.

being the obvious place to start.
So if the emphasis today needs to be less on being nice to everyone, and more on getting something done, with whom should the Franco-German couple first syndicate whatever blueprint for PESCO they manage to agree bilaterally? Size of defence budget should not be a determinant – but it can be an indicator. Only five member states spend more than $10 billion annually on defence, and therefore account for the lion's share of European spending. Take the United Kingdom out of the calculation and France, Germany, Italy, and Spain together provide 69 of every 100 euros spent on defence in Europe. So the first move by Paris and Berlin must be to bind in Rome and Madrid.

A few years back, Poland would have been an obvious next pick. But, since we have mentioned solidarity and shared values – surely both fundamental to defence cooperation – Warsaw, and Budapest, should be left on the bench for the time being. So the trick will be to devise a set of criteria and commitments that opens the door to valuable niche contributors such as the Swedes, or Dutch, or Finns, but keeps the initial group to a manageable eight or nine members, at most. And if that proves too tricky, then just start with four. Other member states can and should be drawn in later, once the new arrangements are up and running and the culture of actually doing things has been established. The whole point of pioneers, after all, is to blaze a trail for others to follow.

Opportunities for real progress on European defence do not come around that often. Unless the present opportunity is seized – that is, unless Paris and Berlin get PESCO off the ground in the next 12 months – we may be in for another decade's wait. Time for those pioneers to move on out.

Anthony Dworkin

Europe’s war on terror

Over the last five years, European Union member states have undertaken a series of military campaigns against terrorist groups outside their borders.[1] These actions, in the Sahel, Iraq, and Syria, represent a major new direction in European security policy. In the years after 9/11, while the United States conducted a global war against al-Qaeda, EU member states largely stayed aloof. But changes in the nature of the terrorist groups in the regions surrounding Europe have prompted a change in the European response, leading to a new wave of European counter-terror wars.

The biggest change that terrorist groups have undergone is a shift towards controlling territory. Al-Qaeda, under Osama bin Laden, was hesitant about any move to set up governing regimes. But in the wake of the turmoil that has spread across the Middle East and northern Africa since 2011, the Islamic State group and various al-Qaeda affiliates have seized control of large parts of several countries. It was the spectre of these ‘safe havens’ not far from European shores that drew EU member states into military action to roll back the territory under the sway of terrorist groups. France’s intervention in Mali in 2012 was the first of these operations, and the wide European involvement in attacks on ISIS in Iraq and Syria represents their fullest development.

Europe’s move into counter-terror war was improvised rather than strategically planned. In both Mali and Iraq, military action was launched quickly to halt the momentum of advancing armed groups. The result is that there has been little systematic thought about the implications of these military actions. It is now a good moment to take stock of what they have achieved and of the unresolved questions that surround them, since European countries seem unlikely to stop mounting such campaigns any time soon.

Militarily, the campaigns by EU member states and their coalition allies have achieved some notable results. Extremist groups no longer hold territory in northern Mali, and the area controlled by ISIS in Iraq and Syria has shrunk dramatically. Operations to recapture ISIS’s last major urban strongholds in Mosul and Raqqa are under way. These successes derive from the fact that air attacks against the groups involved have been combined with ground operations, normally conducted by partner countries.

[1] This paper has been adapted from: Anthony Dworkin, “Europe’s new counter-terror wars”, the European Council on Foreign Relations, 21 October 2016, available at http://www.ecfr.eu/publications/summary/europes_new_counter_terror_wars7155.

Counter-terror activities of main European actors across all theatres

Member state	Airstrikes	Direct support*	Training	Weapons provision	Peacekeeping
Belgium	✈	🔭	👢		UN
Denmark	✈	🔭	👢	🔫	UN
France	✈	🔭	👢	🔫	UN
Germany		🔭	👢	🔫	UN
Italy		🔭	👢	🔫	UN
Netherlands	✈	🔭	👢		UN
Poland		🔭	👢		
Spain		🔭	👢	🔫	
United Kingdom	✈	🔭	👢	🔫	UN

* Direct support includes measures such as reconaissance, refueling and transport assistance.

But these successes at the same time testify to the limits of what military action against terrorist groups can achieve. In Mali, jihadist groups have been dispersed across the Sahelian desert, but they remain capable of launching deadly attacks; terrorist incidents have actually increased in the region as the groups shift away from conventional military operations. In Libya, where the US took the lead and European countries were less involved, ISIS was driven out of Sirte but is regrouping in the country's south. These groups are opportunistic and adaptive, able to shift easily between terrorism and insurgency. As fighters become more mobile and spread across ungoverned spaces, Western countries have increasingly resorted to targeted strikes that have a 'whack-a-mole' quality: they can kill individual fighters, but not erase terrorists' base of support.

The danger here is that Europe may prioritise military action – which is comparatively straightforward and shows the public that something is being done – over the harder and longer-term effort to resolve underlying conflicts or governance failures that allow terrorist groups to implant themselves. Admittedly, solving the problem of regional exclusion in Mali – or, after the capture of Mosul, sectarian divisions in Iraq – is a much greater challenge than dropping bombs on terrorist fighters, and likely to unfold over the course of several years. But without a serious effort to achieve these goals, military action could become an open-ended process of merely trying to keep a lid on the problem.

Directed against groups that combine terrorism with more conventional military operations, Europe's counter-terror wars have also been hybrid in nature. Along with operations to recapture territory or support local ground forces, they have in some cases involved targeted strikes against individual enemy fighters. France and the United Kingdom have conducted such attacks directly and also provided information to the US to use in drone strikes. Among the targets have been figures such the British ISIS members Reyaad Khan and Mohamed Emwazi (also known as "Jihadi John") and the French recruiter and attack planner Rachid Qassim, killed by the US in Iraq in February 2017. It was recently reported in the American press that France has provided Iraqi soldiers with a hit list of French nationals fighting for ISIS to hunt down and kill as they recapture ISIS-held territory.

These operations highlight an additional complexity of European military action against ISIS: it takes place in a context where the boundary between the external and internal dimensions of counter-terrorism has been blurred. Fighters train in Iraq and Syria to conduct attacks on European soil, or manipulate local recruits through a process of 'remote control' plotting. Yet European countries operate on the basis of a supposedly clear division between military action overseas and law enforcement at home. This leads to anomalies – such as France sending an aircraft carrier to the Middle East after the Nice truck attack, conducted by a French resident on French soil. And it leads to legal and moral grey areas – as with the above-mentioned suggestion that France is encouraging the killing of ISIS fighters in Iraq before they can return to French territory.

The effort against terrorist groups overseas and radicalisation at home is one where the EU and its member states are still elaborating their responses. It is one of the most serious security challenges that Europe faces. As regards the external dimension, the balance between military action and a more comprehensive political approach needs careful assessment. And there is still work to be done in defining the legal and moral framework for military operations against amorphous non-state groups that operate transnationally and move seamlessly between insurgent activity on the ground and orchestrating terrorist attacks at long distance.

Ulrike Esther Franke

A European approach to military drones and artificial intelligence

When people hear the word 'drones', they think of targeted killings and the United States. They picture the "Predator" or the "Reaper", the world's most notorious drones, armed with the equally notorious "Hellfire" missiles. They do not generally think of intelligence, surveillance, and reconnaissance systems (ISR), of small 'toss-in-the-air' drones, or of Europe.

This view is as widespread as it is wrong. As of 2017, 90 countries around the world have military drones in their arsenals and 11 states have armed drones. The overwhelming majority of drones are small, unarmed, and used for ISR. All European states but three have military drones, mainly unarmed ones.

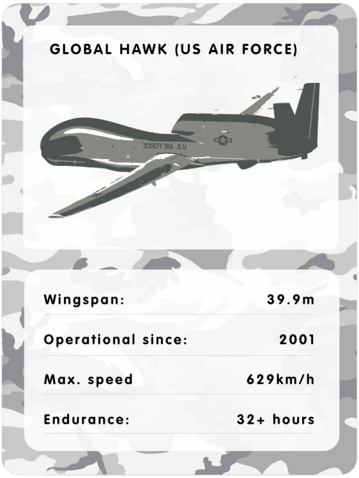
Modern drones have been deployed on battlefields for over a decade.[1] But there is no reason to believe that we have found the best way to use them yet. The use by the US of armed drones for targeted killing in places such as Pakistan, Yemen, or Somalia represents only one way of using drones – but it is the one that has received all of the attention. The European drone debate, from its beginning, has been unduly influenced by the US experience. And despite this attention, the European Union has not succeeded in devising a common stance on US drone use.[2]

Europe's reductive approach to drones has caused it to unnecessarily constrain its thinking in two ways:

First, it has led policymakers to overlook the role of unarmed drones. Armed drones certainly have their place in military operations, but my research shows that from an operational perspective, unarmed drones – which provide levels of ISR never seen before and at the lowest levels of the military hierarchy – may be at least as revolutionary as armed drones, since they can make a substantial difference in military operations and save lives.

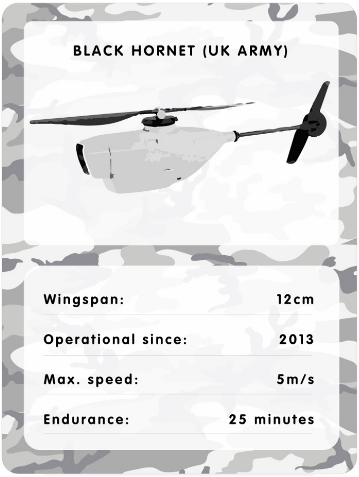
[1] The Soviet Union had drones, the US used them in the Vietnam War, and Israel in the Yom Kippur War and in 1982 in Lebanon. But drones really came of age around the year 2000, when the technology reached maturity and positive experiences in Kosovo pushed European countries and the US to invest more. 9/11 and the wars on terror dramatically increased demand for and investment in the military technology.

[2] Anthony Dworkin "Drones and targeted killing: defining a European position", the European Council on Foreign Relations, 3 July 2013, available at http://www.ecfr.eu/publications/summary/drones_and_targeted_killing_defining_a_european_position211.



GLOBAL HAWK (US AIR FORCE)

Wingspan:	39.9m
Operational since:	2001
Max. speed	629km/h
Endurance:	32+ hours



BLACK HORNET (UK ARMY)

Wingspan:	12cm
Operational since:	2013
Max. speed:	5m/s
Endurance:	25 minutes

Second, more generally, it is a terrible idea to focus on only one specific usage of a new technology. Generations of scholars have dedicated their careers to finding out what makes military technology ‘revolutionary’. While many different explanations have been brought forward, there is universal agreement on one point: it is not (just) about the technology, it is about how you use it. What makes a technology truly ground-breaking, effective, and possibly revolutionary, is policy and doctrine.

The classic example for this is tank warfare. Tanks had been on the battlefield since 1916, but it was the Wehrmacht’s introduction of independent armoured divisions and their innovative use of radio in the second world war that allowed them to rapidly break through enemy lines. This was what made tanks revolutionary.

European countries should end their fascination with American drone warfare and consider how drones can best suit the needs of their own armed forces. This will help to focus the debate on how best to use the technology, and what capabilities to invest in.

There is a window of opportunity now that Europe should take advantage of. European armed forces have largely returned from missions during which they had their first real experiences of using drones, such as in Afghanistan and Iraq, or are currently using them in ongoing operations in the Sahel/

Mali and Syria.[3] Most countries bought drones as an urgent operational requirement, but European armies are still thinking about where they fit in. From a military doctrine point of view, this means that now is an appropriate time to step back, evaluate, and invest.

While armed forces in each European country must assess individually what type of drone use fits them best, the EU should use the new EU defence fund for investment in a common, small, and robust European drone.

Drones are already high on the list of European priorities: France, Greece, Italy, Spain, Sweden, and Switzerland are working on the "nEUROn" drone; Germany and Spain on "Barracuda"; the UK is developing the technology demonstrator "Taranis"; France and the UK in 2016 agreed to invest £1.5 billion in a new combat drone; France, Italy, and Germany began a drone partnership in 2015, and NATO is acquiring five US "Global Hawk" drones.[4]

But while European investment in future technology is to be welcomed, these projects all face common problems:

1. despite some of them having begun many years ago, there is little to show for the investment;

2. as expensive, high-tech combat systems, it is unlikely that they will be needed by many European forces;

3. because they are high-tech and armed, they are not easily exportable.[5]

It would be of much more immediate use to invest in a common European small, robust, ISR drone system (maybe optionally armed) and related swarm technology that enables them to work collectively. Small ISR drones have more than proven their worth and are being used around the world. Indeed, their continuous demand in Europe and abroad is guaranteed because of their value in ISR activities. At this point, the market is dominated by the US "Raven" (and indigenous systems). But the Raven is not without its problems. Raven drones were recently hacked by Russian forces within hours of being sent above the battlefield in eastern Ukraine. Ukrainian forces had to resort to crowdfunded drones instead.[6]

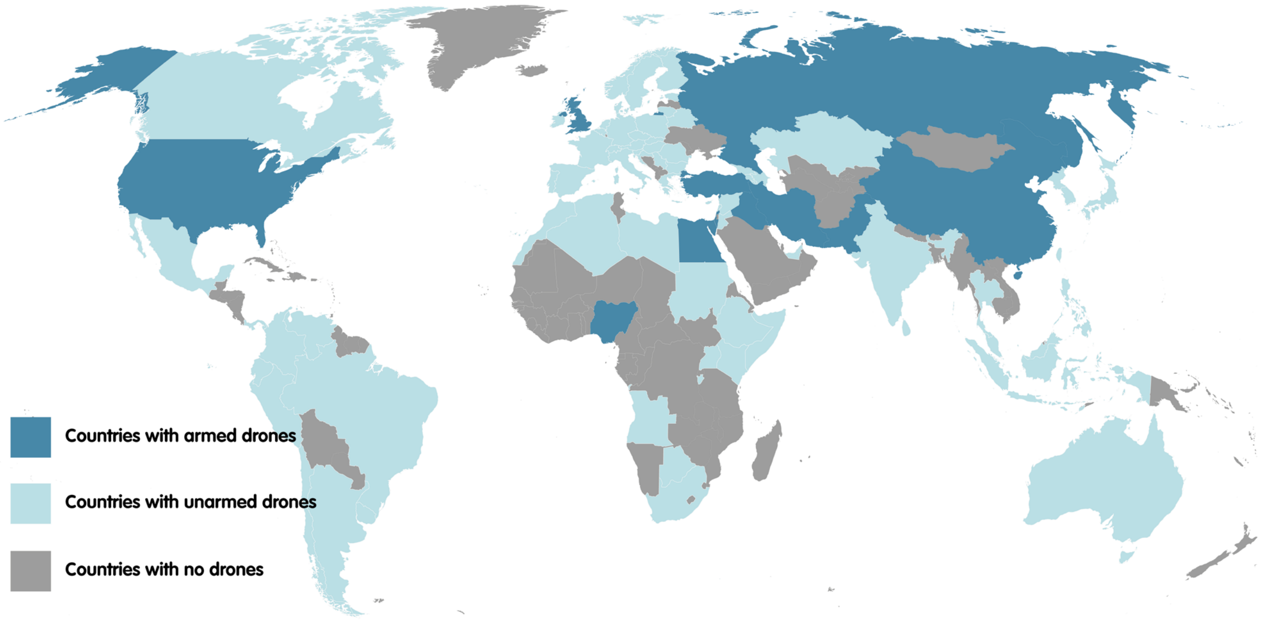
[3] Denmark, Czech Republic, Germany, Italy, and the UK used drones in Afghanistan; the UK and Italy used drones in Iraq; France, Germany, and Sweden have, or are, using drones in the Sahel region; and the UK is using drones in Syria.

[4] On European drone project see Ulrike Franke "U.S. Drones Are from Mars, Euro Drones Are from Venus, War on the Rocks, 19 May 2014, https://warontherocks.com/2014/05/u-s-drones-are-from-mars-euro-drones-are-from-venus/.

[5] Europeans may be reticent to export high-tech weaponry and the exports of such systems is restricted by existing export control treaties.

[6] Bjoern Mueller, "Krieg fuehren per Crowdfunding", FAZ, 11 March 2017.

Global drone proliferation (2017)


■ Countries with armed drones
■ Countries with unarmed drones
■ Countries with no drones

There is a clear opening for a more robust small European drone system. It would be of enormous operational advantage if European forces had common systems, ensuring interoperability, common training, and much more.

Focusing on smaller drones that can work together as a swarm would also put Europe in a strong position regarding the next potential revolutionary military technology – artificial intelligence (AI). AI is not solely (or even primarily) a military technology, which is why Europe's approach to AI cannot be exclusively military. But AI will be part of the future of warfare, initially through autonomous weapons that can find and engage targets independently and operate in swarms. Drones and other unmanned systems will be the first to be affected – indeed they already are being affected.[7]

It is crucial that Europe does not repeat the mistakes it made with drones when it comes to AI. Chasing developments in the US instead of thinking strategically about a European position and use for the technology would be a grave error. Europe has an opportunity to ensure that the next, AI-powered drone system on everyone's lips is European-made.

Armed drone user	System built by
China	China
Egypt	China
Iran	Iran
Iraq	China
Israel	Israel
Nigeria	China
Pakistan	Pakistan
Russia	Russia
Turkey	Turkey
UK	US
US	US

[7] Ulrike Franke, „Automatisierte und autonome Systeme in der Militär- und Waffentechnik“, Aus Politik und Zeitgeschichte APuZ, August 2016.

Stefan Soesanto

Cyber attacks: Understanding the basics

Rarely does a week go by these days without a 'cyber attack' making the headlines across the globe. It may be the massive WannaCry ransomware campaign that infected 300,000 systems in more than 150 countries, the hacking of Qatar News Agency which led to numerous fake postings on the nation's official media platform, or Pyongyang's targeted phishing campaign against members of the United Nations Security Council's North Korea Sanctions Committee. Typically, in the public discourse all these incidents are generically termed 'cyber attacks' with little to no distinction between them.

To put this into perspective, imagine a world in which every malicious act – no matter how insignificant – is classified as 'murder.' And now think about how this would affect your sense of security.

Indeed, one of the elemental challenges when it comes to cyber security and cyber defence is that, as the NATO Cooperative Cyber Defence Centre of Excellence eloquently describes it, "there are no common definitions for cyber terms — they are understood to mean different things by different nations/organisations."[1]

The most prominent example of this problem breaking to the fore occurred in September 2015 when James Clapper, then the United States' director of national intelligence, testified before the US House Intelligence Committee. Clapper told lawmakers that the intrusion into the US Office of Personnel Management (OPM) network – and the resulting theft of personal information belonging to 21.5 million current, former, and prospective government employees – was not a cyber attack, because "there was no destruction of data or manipulation of data. It was simply stolen. That's a passive intelligence collection activity—just as we do."[2] Lawmakers could not believe their ears and vehemently argued that a refusal to call the OPM hack an attack would minimise the gravity of the event and leave the US open to similar incidents if there was no forceful response.

[1] "Cyber definitions", NATO Cooperative Cyber Defence Centre of Excellence, available at https://ccdcoe.org/cyber-definitions.html.

[2] DNI, NSA Seek Offensive Cyber Clarity; OPM Not An 'Attack', Breaking Defense, 10 September 2015, available at http://breakingdefense.com/2015/09/clapper-rogers-seek-cyber-clarity-opm-not-an-attack/.

30

nations are developing offensive cyber capabilities

2

cyberattacks have caused physical damage

Yet, Clapper was right. The most adequate legal definition of what constitutes a cyber attack can be found in the Tallinn Manual on the International Law applicable to Cyberwarfare, which describes it as: “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”[3]

To date, only two cyber attacks have successfully cleared this physical threshold. The first is the infamous Stuxnet worm which was deployed against the Iranian uranium enrichment plant in Natanz back in 2007-2008. The second is a much lesser known cyber attack against an unnamed German steel mill in 2015 which resulted in “massive—though unspecified—damage.”

Several other cyber incidents have come very close to crossing this threshold. For example, the Shamoon breach at Saudi Aramco during Ramadan in 2012, “partially wiped or totally destroyed the hard drives of 35,000 Aramco computers.”[4] The incident even forced then US secretary of defence Leon Panetta to note that Shamoon is “one of the first [pieces of malware] we’ve seen that can actually take down and destroy computers [...] to the point that they had to be replaced.”[5]

[3] “Tallinn Manual 2.0”, NATO Cooperative Cyber Defence Centre of Excellence, available at https://ccdcoe.org/tallinn-manual.html, p.106.

[4] “Inside the aftermath of the Saudi Aramco breach”, Dark Reading, 8 August 2015, available at http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676.

[5] “DOD News Briefing with Secretary Panetta and Gen. Dempsey from the Pentagon”, US Department of Defence, 25 October 2012, available at http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5143.

Equally disturbing were the intrusions into the Ukrainian power grid in late 2015, which cut off electricity for approximately 225,000 Ukrainians in the middle of December. According to E-ISAC, the breaches in Ukraine are "the first publicly acknowledged incidents to result in power outages."[6]

Getting terminology right is immensely important in the cyber domain, because calling everything by the same name (1) undermines the public's sense of cyber security, (2) blurs the lines between acts of war and criminal activities, (3) and disguises the greater dangers of exploit proliferation, misattribution, and collateral damage.

Code and exploit proliferation is a growing issue. Roel Schouwenberg, former senior analyst at Kaspersky Lab, explains that, "regular cybercriminals look at something that Stuxnet is doing and say, that's a great idea, let's copy that."[7] But it is not only cybercriminals and script kiddies that are in the business of repurposing chunks of code – nation states are too.

After 2007-2008, sophisticated Stuxnet-like trojans, such as Duqu, Flame, and Gauss, popped up in the wild, wreaking havoc across the Middle East and making their appearance in Europe as well. The fallout of Shamoon progressed similarly: dormant for four years, researchers at Kaspersky Lab observed three waves of Shamoon 2.0 deployments against Saudi infrastructure, starting in November 2016. According to the Saudi Ministry of the Interior, Shamoon 2.0 wiped approximately 1,800 servers and some 9,000 computers in 11 organisations. Amid the new onslaught, Kaspersky Lab also discovered an elaborate new disc-wiper malware, now dubbed 'StoneDrill'. To the surprise of many, given previous trojans' propensity to remain in the Middle East, StoneDrill made its first foray outside that region by hitting a petroleum company in Europe.[8]

What danger does this pose to Europe?

Despite the assertion of Thomas Rid, professor in security studies at King's College London that "Cyberwar will not happen", nation states and cybercriminal groups are already waging a silent conflict in the dark across the web. Europe should be particularly concerned with Russian activities. In fact, all of the Russian Advanced Persistent Threat (APT) actors, such as

[6] "Analysis of the Cyber Attack on the Ukrainian Power Grid", EISAC, 18 March 2016, available at https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, p. vi.

[7] David Kushner, "The real story of Stuxnet", IEEE Spectrum, 26 February 2013, available at http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[8] David Goodin, "This hard drive will self destruct. Data-wiping malware targets Europe", ArsTechnica, 3 June 2017, available at https://arstechnica.com/security/2017/03/this-hard-drive-will-self-destruct-data-wiping-malware-targets-europe/.

groups that are sponsored by a nation state or are nation state agencies, are primarily targeting European businesses and governments.

APTs like Fancy Bear and Cozy Bear (controlled by Russia security agencies the GRU and FSB respectively) – now well-known household names due to their central role in Russian interference in the 2016 US presidential election – have penetrated numerous European institutions, ranging from NATO and the Organization for Security and Co-operation in Europe to France's TV5Monde and the German parliament. The Sandworm Team, another Russian APT actor, not only caused a powercut for 225,000 Ukrainians in late 2015, but also breached western European government agencies, Polish energy firms, and French telecommunication companies. It even targeted attendees at the 2014 GlobSec Forum in Bratislava.[9] Equally, the Russian APT Waterbug predominantly compromised government and media websites in Europe. According to a 2016 assessment by security software company Symantec, the top four countries targeted by Waterbug are France (19 percent), Germany (17 percent), Romania (17 percent), and Spain (13 percent). The US accounted for only 4 percent of Waterbug activities world-wide.

The Democratic National Committee hack should have been a wake-up call for Europe. For far too long Europe has turned a blind eye to the persistent Russian threat in cyber space, and has left the US to deal with the issue alone on the international stage. Currently, there is little public discourse in Europe, nor is there even any foreign policy response in the making which takes into account the myriad Russia-linked APT intrusions that have breached European governments, companies, and individuals over the past five years. It is time for European policymakers, law enforcement agencies, and the intelligence community to step up to the plate, and defend the continent in cyber space.

In light of this, the one-and-a-half day Cyber WarGame, held in Brussels on 19-20 June by the European Council on Foreign Relations and Microsoft, was a first step to helping sharpen this understanding. It brought together government officials from across the EU28, to explore escalation dynamics in cyberspace, define national red lines, map norms of acceptable state behaviour, and analyse possible responses across the threat spectrum in an environment of uncertainty.

[9] "Russian Cyber Espionage Campaign - Sandworm Team", the *Washington Post*, available at https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National-Security/Graphics/briefing2.pdf.

Manuel Lafont Rapnouil

Signal, constrain, and coerce: A more strategic use of sanctions

It is a well-known fact that over the last few decades, the European Union has intensively resorted to sanctions. It is not just that, quantitatively, Europe has multiplied the number of its sanctions regimes, but the measures have also become more varied and targeted. About 35 sanctions regimes are currently in place. These range from asset freezes and travel bans to arms embargoes to restrictions on financial transactions – against a diversity of entities, whether individuals, non-state organisations such as terrorist groups or major powers. Sanctions have consequently gained relevance, with these "restrictive measures" (as the EU likes to call them) having played or still playing a key role in some of the EU's biggest security policy successes (such as the nuclear deal with Iran), in its relations with major partners (Russia and China) or in some of the most nightmarish crises it faces (like Syria). But with this success, criticisms have also grown, both on the effectiveness of sanctions and on their strategic nature.

Since the 'sanctions decade' of the 1990s, which saw the United States, the United Nations, and the EU resort to sanctions on a much more systematic basis, the hopes for a 'new world order' built around collective security and non-use of force have been dashed. Yet, far from disappearing, sanctions continued to be used. They became more sophisticated too, developing from broad embargoes to targeted financial sanctions and increasingly targeting individuals rather than whole countries or entities. Still, their success is disputed. The merits of sanctions – as an adaptable tool, less heavy and costly than the use of force, possibly targeted enough to allow for the continuation of relations, and even some trade – are what lead many to suspect that they have become a tool of choice by default, an easy way for Europe to react to a variety of situations (such as nuclear proliferation, conflicts, terrorism, and human rights violations) without always being strategic and serious about follow-up.

This discussion has been further heightened with continued doubts about their usefulness. Challenges have come from humanitarian, economic, or legal arguments. But the most delicate debate is about effectiveness. The fact that few sanctions regimes ever get abolished while new ones keep being added may also appear as a testimony to their inability to solve the problem they respond to. Yet, the question is often more complex than we see. In Iraq in 2003, sanctions were used to prevent Saddam Hussein from pursuing his weapons of mass destruction programmes, but the post-9/11 US demanded a degree of certainty about their effectiveness that they did not think UN inspections could ever provide. On Iran, sanctions were decried for years since they hadn't resulted in Iran halting its nuclear programme.

Too often, people look at the discussion about the effectiveness of sanctions through the prism of how decisive an impact on state behaviour these measures have compared to their drawbacks, whether for our economies or for local populations. Research has identified the conditions – such as the size of the sanctioned country, the intensity of the bilateral relationship, preference for short-term consequences, ability to universalise the sanctions, speed and unity in adoption – which determine the impact sanctions can have.

But effectiveness is first and foremost linked to the balance between the sanctions' three possible goals: to signal, to constrain, and to coerce. First, 'signal' expresses determination, i.e. it warns of possible further action, and therefore engenders deterrence, including vis-à-vis others. Second, 'constrain' seeks to prevent the sanctioned state or entity from pursuing its course of action, through measures from weapons embargoes to dual-use technology prohibitions to financial measures. Third, 'coerce' imposes costs on the sanctioned state or entity to build up leverage for negotiations. Effectiveness should always be assessed against which of these objectives are pursued.

More importantly, sanctions are not a strategy by themselves, but a tool. Their effectiveness does not only depend on whether they are tailored to the goals identified but on whether they are credible. This implies that sanctions are situated within a broader political strategy that, in some cases, can include the use of force – if only through robust peace operations. Sanctions also have to be adjusted to the evolution of the situation on the ground – not just when it comes to adoption of further sanctions or their gradual lifting, but also according to a close follow-up of their implementation and impact. The perpetuation of sanctions without any change on the ground and adjustment in the measures is usually a recipe for diminishing impact, if not for sanctions erosion: just as with any coercive policy, sanctions too need an exit strategy.

The EU and its member states need to use sanctions more strategically, and to organise themselves accordingly to make sanctions more effective. These are some areas on which Europe should focus:

- While each case requires a tailored approach, Europe should spend more time on its strategic approach to sanctions. In a striking fashion, and in spite of their growing importance, neither the EU Global Strategy, nor most member states' defence or national security strategies, have really dug into this issue. Deep thinking on sanctions would help build consensus on how to use them, under which conditions, and to what end. It could even provide a way forward for making European sanctions more effective.

- In the Brexit debate, sanctions are rarely mentioned as an important topic. But the United Kingdom is one of the countries whose policy thinking on sanctions is most advanced, and has often been instrumental in ensuring EU sanctions have some impact. Brexit will therefore come with a number of consequences for both sides, only further underlining the fact that future UK-EU relations on security issues will not be limited to defence matters. It would certainly be suboptimal if EU-UK relations do not include a political dialogue on sanctions, and how they are designed, leveraged, implemented, and adjusted.

- In any case, Europe will benefit from better collective and national organisation on sanctions. For instance, more intelligence dedicated to sanctions, as well as specific monitoring of their impact, would be helpful when adopting and revising the regimes, as well as in terms of ensuring proper implementation.

- With the distribution of sanctions-related costs having become a growing topic of intra-EU discussions, Europe also needs to improve its management of these consequences, including further developing mechanisms designed to compensate the hardest-hit economic sectors.

Finally, Europe needs to adjust to the way in which the world has changed. The current state of transatlantic relations may end up testing both Europe's ability to maintain strong sanctions without the US and to shield its economic activities from US sanctions not coordinated with Europe, as transatlantic differences on Russia or Iran exemplify. The rise in the use of sanctions by other powers like Russia, or regional organisations such as the African Union, only confirms the need for Europe to think about sanctions more strategically.

Gustav Gressel

Russia’s quiet military revolution

Russia has surprised the West with its military capacity twice in the past three years.[1] First, in Ukraine, Russian armed forces overturned Western assumptions about their inefficiency with a swift and coordinated ‘hybrid war’, combining subversion and infiltration with troop deployment to gain an early military advantage. Then, in Syria, Russia used military force outside the borders of the former Soviet Union for the first time since the end of the cold war.

The current Russian leadership has never accepted the post-1989 European order, including the norms, rules, and conventions agreed by the last generation of Soviet leadership. The Kremlin does not seek incremental changes to the current order but aspires to create a totally new one. It regards post-Soviet borders as something to be revised – with military force, if necessary. Until 2014, Russia was not able to underpin this desire for a revision of the European order with force.

However, Russian military thinkers and planners have been creative in trying to overcome the multiple disadvantages of the Russian military apparatus vis-à-vis its Western counterparts. They have implemented far-reaching military reforms to create more professional and combat-ready armed forces that can swiftly deploy abroad, backed by expertise in non-conventional warfare tactics such as subversion and propaganda.

While in the past the Russian armed forces needed years to gear up for military confrontation, they now have the ability to react quickly and strike without warning. However, the Russian authorities planned their military reform in three phases, starting with the reforms that would take the longest to produce results. First, increasing professionalism by overhauling the education of personnel and cutting the number of conscripts; second, improving combat-readiness with a streamlined command structure and additional training exercises; and only third, rearmament. The initial stages were designed to ensure that existing equipment was ready to use, and to make the organisation that uses it more effective and professional. Indeed, to successfully intervene in Russia’s neighbourhood, Moscow does not necessarily need the latest cutting-edge defence technology. Rather, such

[1] This paper has been adapted from: Gustav Gressel, “Russia’s quiet military revolution and what it means for Europe”, the European Council on Foreign Relations, 12 October 2015, available at http://www.ecfr.eu/publications/summary/russias_quiet_military_revolution_and_what_it_means_for_europe4045.

interventions would have to be precisely targeted and quickly executed to pre-empt a proper Western reaction. But Western analysts' focus on the fact that the rearmament stage of the reforms is incomplete and delayed has caused them to overlook the success of the other two stages. These have already given Russia a more effective and combat-ready military, as demonstrated by its fast and coordinated intervention in Ukraine.

Russia's military efforts are embedded in a multi-pronged drive to overwhelm, subvert, and subdue the opposing society. This drive is much more ruthless and effective than the West's 'comprehensive approach' – the coordination of civilian and military efforts in conflicts and crises. As leading Russian analysts stated at the 2012 Valdai Discussion Club: "The distinction between 'civilian' and 'military' segments of society is disappearing. The aim of a military campaign is to impact not only the enemy army, but also its society, understood in terms of its cultural as well as its physical aspects. This trend makes it necessary to conduct joint 'civilian-military' operations, rather than purely military ones."[2]

These efforts are aided by Russia's paramilitary and non-military forces. In the Russian Federation, the Ministry of Interior has about 170,000 men in ready-formed and trained paramilitary units at its disposal to tackle domestic unrest, terrorism, and border violations.[3] There is no need for the armed forces to supplement them in case of an emergency. Similarly, natural disasters and humanitarian aid are taken care of by the Ministry for Emergency Situations, which also has its own troops. These paramilitary and non-military forces would play an important role if Russia carried out a full invasion of one of its neighbours. Both services were mobilised in April 2014 when the Russian military was preparing its assault on Ukraine.

In Ukraine, Russia has engaged not only in a conventional war but also in wars of subversion and propaganda, and in multiple disinformation campaigns at home and abroad. There is a trade and financial war going on, in which Russia tries to weaken the Ukrainian economy by cutting off imports, selectively harming entrepreneurs that support the new government, and corrupting others. This operates alongside a multi-pronged campaign by political representatives, intelligence services, and Russian businesses to undermine European support for Ukraine.

[2] Mikhail Barabanov, "Changing the Force and Moving Forward After Georgia", in Colby Howard and Ruslan Pukhov (eds), *Brothers Armed: Military Aspects of the Crisis in Ukraine* (East View Press: Minneapolis, 2014),

[3] "The Military Balance 2015", The International Institute for Strategic Studies (Routledge: London, 2015), p. 197 .

Russia's military modernisation and re-emergence as an expansionist, revisionist actor on Europe's eastern borders has profound strategic consequences for Europe. Little that was true for Europe's security in the 1990s and early 2000s is still valid. However, the situation Europe faces today is not a repetition of the cold war. While there is again a systemic and ideological conflict between the democratic West and a revanchist Russia, Russia has neither the will nor the capacity to compete with the West on a global scale. But even if Russia is unable to shape world politics, it may be able to spoil it. And, as its expansionist aims threaten the very existence of some of the EU's eastern member states, the Russian threat will be a much more serious challenge for Europe than for anybody else on the planet.

The European defence establishment has until now been confident that Russia's armed forces could be checked, at least in qualitative terms. However, this qualitative advantage applies to few European NATO members. France, the United Kingdom, and Germany have armed forces of superior quality to Russia's, but issues of deployability, readiness, and quantity of ammunition could put this qualitative advantage into question. Russia could now overwhelm any of the countries in the post-Soviet sphere if they were isolated from the West, but it lacks the capacity for effective long-term military action further afield, such as in Syria.

Russia is clearly preparing itself for offensive operations. It could exploit the weaknesses of its Western neighbours to achieve strategic surprise, but big risks and uncertainties for Russia are attached to these options. Much will depend on how Western leaders react to Russian provocations in the case of a crisis. Hence the challenge is more political than military: only credible political coherence, solidarity, and deterrence can prevent military adventurism. Whether such adventurism will hit the European periphery or Europe itself will largely depend on the state of Europe's defence.

Europe should develop a united political response to Russian expansionism, including a coordinated position on nuclear deterrence, while preparing for hybrid scenarios.

The initial reaction to an unconventional, subversive Russian military operation should resemble stabilisation or crisis intervention rather than traditional defence. Rapid and high-quality deployment would be more important than striking power for spearhead forces, because they first have to deny unconventional forces access to critical infrastructure and administrative facilities. Close cooperation with non-military state authorities would be essential.

In the second phase of the response to Russian aggression, Europe would have to deploy forces with sufficient striking power and sustainability to deny Russian forces the option of an armed incursion, or, if that has already happened, to stop and repel it.

Given the strong transatlantic dimension of European defence, especially the nuclear aspect, it seems obvious that NATO is the primary arbiter of a new European defence policy. But it would be unwise to forget the EU's role. Many of the EU's assets developed for crisis response (such as special police or Gendarmerie forces, and civil administration assets) will be useful in a hybrid scenario, either in the European neighbourhood or in the EU itself.

Last but not least, Article 42 (7) of the Treaty on European Union, which guarantees the security of member states, is still a reserve framework in case NATO decisions are blocked by obstructive member states. It also covers Finland and Sweden – both non-NATO members facing an increasingly assertive Russia. The exploration of common defence preparation with these Nordic non-aligned members will be important.

Mattia Toaldo

Libya: Security through politics

Libya has gradually emerged as one of Europe's worst headaches. After the fall of Muammar Gaddafi in 2011, public opinion and opinion-makers alike considered Libya to be riven with chaos, anarchy, and violence; it was known as a source of uncontrolled migration and terrorism. Yet, despite these concerns, Libya rarely made it into high-level conversations between national leaders and little effort was made to help steer the country in the right direction. This changed in late 2014, when the threat of an Islamic State group foothold close to European shores and the continuing anarchy put the north African country back on the list of European worries.

2012 and 2013 were years of fatal mistakes by the post-Gaddafi leadership. First, militias were given government salaries, and they then quickly moved to take control of what was left of government institutions. Second, no reconciliation process was launched while a particularly strict lustration law effectively excluded a large portion of the population from politics and the civil service. This resulted in increasing levels of anarchy as the country lacked a proper security sector while instead having a collection of rival militias on the government payroll. Meanwhile, the lack of political reconciliation led to increasing political divides. This eventually resulted in the building of rival armed coalitions in mid-2014: the anti-Islamist and Egypt-backed Operation Dignity, led by renegade general, Khalifa Haftar, and the radical, pro-Islamist Libya Dawn militia, which eventually took control of Tripoli.

After the Libyan government left the capital, a rival government was created in Tripoli by Libya Dawn, and the country slipped into a low-intensity civil war that is ongoing today. At the same time, ISIS gradually expanded its foothold, establishing territorial control of over 200 kilometres of Mediterranean coastline in the summer of 2015. By this point, containment and neglect of Libya were no longer an option for European policymakers.

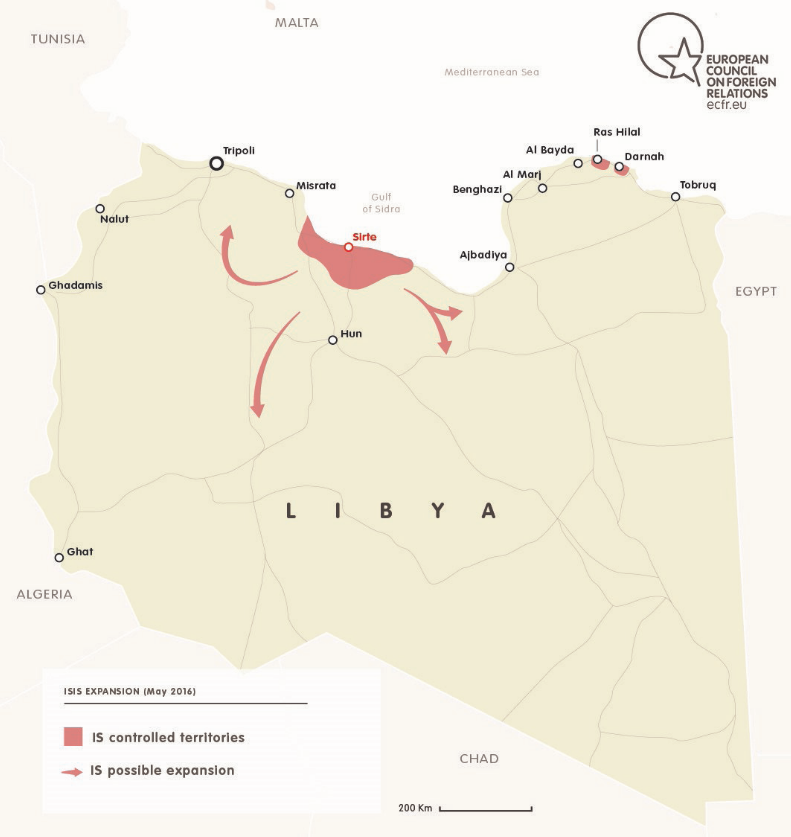
European efforts, often in conjunction with the Obama administration, went in two directions. First, large European Union member states, including the United Kingdom, France, and Italy converged on the need to prioritise a political process that would lead to the creation of a national unity government. This eventually resulted in the United Nations-brokered Libyan Political Agreement signed in Skhirat, in Morocco, and endorsed by the UN Security Council in December 2015. Second, the US and Europeans supported Libyan anti-ISIS Operation Bunyan al-Marsous with both airstrikes and special forces. An EU naval operation, named Sophia, was deployed to fight people smugglers in the Mediterranean. The EU Border Assistance Mission (EUBAM) was stepped up and became a Common Security and Defence Policy mission – albeit with a very narrow mandate. It was criticised by several EU members.

These combined efforts were not a magic wand but they did achieve some results. There was a reduction of violence almost everywhere except for the city of Benghazi and some other areas. Generally, Libya did not reach the levels of casualties of Syria or Yemen and ISIS's territorial control ended in December 2016, with its fighters either fleeing the territory or dying in combat, dealing a big blow to the organisation's narrative. The internationally recognised government is now based in Tripoli, although two rival governments still exist and implementation of the United Nations-brokered agreement is stalling. Irregular migration is not under control and Europeans are trying to go beyond Libya by working particularly with Niger and other neighbouring countries.

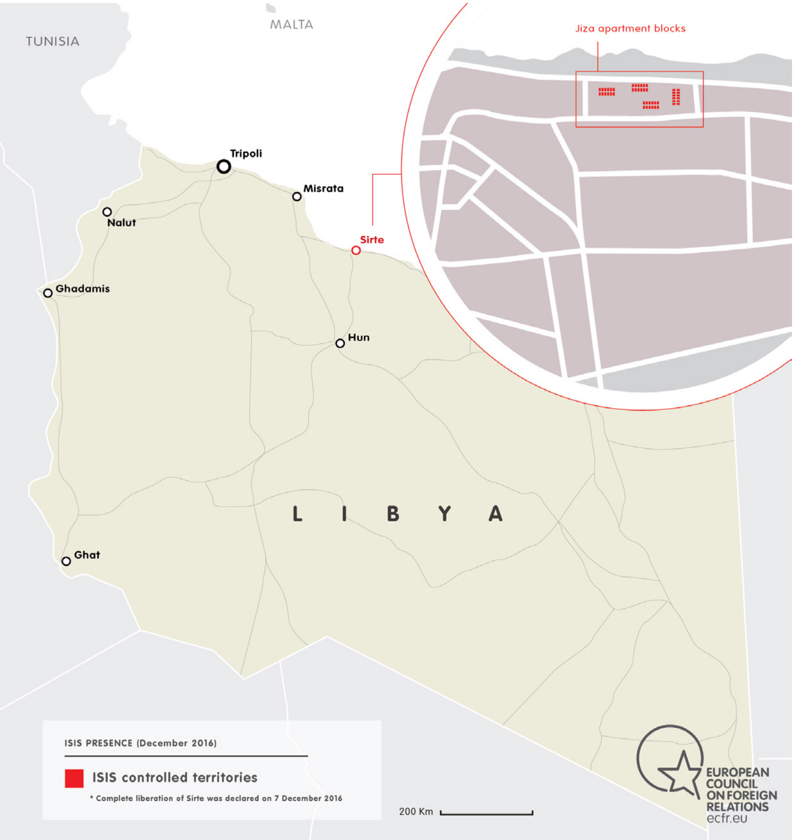
Overcoming these problems will be key both for Europeans and for Libyans. Rebuilding unified governance is essential. It is not simply about having a unity government but also about having a single central bank, a single National Oil Corporation, and ultimately avoiding a situation in which duplicate bureaucracies respond to different governments without actually control the country. Unfortunately, a new and more inclusive political agreement is unlikely to be concluded any time soon as the positions of Haftar and his opponents grow further apart and the regional splits in the Persian Gulf and beyond get deeper and deeper.

For many European governments, it would be easier to find a single interlocutor, whether Prime Minister Fayez al-Serraj in Tripoli, or Haftar, or a combination of the two. But no single actor can control all of Libya, and hence be a reliable partner to address Europe's concerns.

The difficulties of the political process should not lead Europe to adopt a narrow security-driven approach. Libya cannot be dealt with by letting regional powers compete for power and influence while occasionally using air strikes to hit 'the bad guys', as the prevailing approach of the Trump administration seems to be.



Instead, the EU and particularly the most active countries such as France, Italy, the Netherlands, and Malta, should adopt a multi-pronged stabilisation approach. As in many other fields of foreign policy and security, cooperation with the UK, despite Brexit, will be essential. First, the EU or a coalition of member states should push the Libyan parties to reach an agreement to share natural resources in order to eliminate one of the main drivers of conflict and avoid a humanitarian crisis. Europe, as the main buyer of Libyan oil and an important financial partner for Libya, has relevant leverage and interests in this field. For Libyan politicians and businessmen, the threat of an EU asset freeze and travel ban is still highly pertinent. Second, the EU should support municipalities and existing institutions in providing public services. Third, Europe should strengthen, support, and extend local ceasefires to reduce levels of violence and the potential for escalation. Fourth, the


TUNISIA
MALTA
Jiza apartment blocks
Tripoli
Misrata
Nalut
Sirte
Ghadamis
Hun
L I B Y A
Ghat
ISIS PRESENCE (December 2016)
🟥 ISIS controlled territories
* Complete liberation of Sirte was declared on 7 December 2016
200 Km
EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

EU should promote the disbandment of militias and the building of a national army from the bottom up. In this sense, the recent establishment of seven 'military regions' could be an opportunity to build local 'security tracks' through UN and EU mediation efforts.

For every crisis and conflict in the Middle East and north Africa there is always the temptation, in most capitals, to look for the 'ultimate deal' and therefore to push for a political process regardless of its chances of success. But the ultimate yardstick for judging the success of a policy should be how many human lives have been saved and how much it has improved the living conditions of the local population. Stabilising Libya will ensure the country is a less fertile ground for radicalisation and terrorism. At this stage in Libya, the road to achieve that is to focus on stabilisation efforts even in the absence of the 'ultimate peace deal'.

Mathieu Duchâtel

Coming to terms with China’s maritime power

When Europeans think of naval power, maritime security, and China, they think of the militarised artificial islands in the South China Sea. They rightly associate them with legal issues of freedom of navigation and the risk of a clash between the People’s Liberation Army (PLA) and the United States-Japan alliance. Inevitably, this line of thinking leads to the conviction that Europe only has limited means to shape the maritime security environment in east Asia. But the issue of naval power has already moved to areas that present Europe with direct challenges and opportunities.

Europeans should not be surprised when in five years’ time the People’s Liberation Navy (PLAN) docks one of its aircraft-carriers at China’s new naval base in Djibouti, which is currently under construction. While a Chinese bombing campaign in the Gulf or in eastern Africa is unlikely, airstrikes from such a carrier are not completely out of question if the PLA is invited by a sovereign state to intervene militarily, on the model of Russian intervention in Syria, or as part of a multinational coalition with a United Nations Security Council mandate. “Military operations other than war” (非战争军事行动) could put China’s new expeditionary force to use serving the country’s “overseas interests” (海外利益), a term included in Chinese official documents since 2012 and which covers the protection of Chinese nationals and assets overseas.

The possibility of using military power in counter-terror missions has been integrated into China’s toolbox since the December 2015 ‘Counter-Terrorism Law’. With a fleet of three aircraft carriers – and Chinese analysts now openly discussing a future force of six battle groups – China will command a greater number of options to influence international crisis management.

States use aircraft carriers to win naval battles and project air power, but also for deterrence and diplomatic signalling. In the words of a military analyst recently interviewed in Beijing, “carriers are the closest tool to Sun Tzu’s teaching of subduing adversaries without fighting”.[1] One easily imagines the PLAN’s battle group providing a shield to a large non-

[1] Author’s interview with senior military officer, Beijing, May 2017.

combatant evacuation operation. Now a standard response to eruptions of violence overseas where there are large numbers of Chinese nationals, the country has conducted 17 such operations in a little more than a decade. But so far these have all been conducted from relatively safe operation theatres not requiring air superiority.

Aircraft carriers are the most visible side of China's maritime power – the side also played up by the Chinese media as the striking symbol of a 'new normal'. They are part of a massive and ongoing investment in shipbuilding, naval capacities, and marine science and technology. It has been five years since building a "great maritime power" (海洋大国) became a national strategic goal. The upcoming 19th Party Congress this autumn will certainly re-emphasise this objective, further consolidating the status of the PLAN as the key service providing protection to the next phase of China's economic globalisation, characterised by higher levels of foreign direct investment, contracted infrastructure projects, and their associated loans.

In China's official Military Strategy, published in 2015, oceans are a "critical security domain", together with outer space and cyberspace. The document makes clear that the country's maritime security posture has already shifted with "open seas protection" complementing offshore defence. Rumours circulate in China that the country will soon issue its first maritime strategy paper. Some fundamental questions are still subject to much internal debate. How to reconcile Xi Jinping's plans for a Maritime Silk Road linking European and Chinese ports with disputes and risks over maritime boundaries and islands in East Asia? Does China need to choose between being a land power and a sea power? How central will power projection be in the future force structure of the PLAN, by comparison with undersea nuclear deterrence? Should the defence of the Maritime Silk Road determine the future posture of the PLAN?

The question of how to deal with China's changing posture as a global security actor, and the new political options that a powerful navy will offer to Beijing is of crucial importance to Europe. Djibouti is a test case. China's permanent naval presence will allow for a modest increase in Europe-China security cooperation. The European Union is planning to upgrade existing interactions with the Chinese navy, which so far are limited to annual modest joint naval exercises in the Gulf of Aden, and joint escorts of World Food Programme shipments to Somalia. This is likely to remain low profile but a process of engagement with China on operations with a human security dimension is in Europe's interest.

Furthermore, and less immediately obvious, there is a crucial economic dimension to the Chinese naval build-up, and innovation is the key battlefield for Europe. Parallel to spending on the navy, the marine economy is a priority of China's 13th Five-Year Plan. The State Oceanic Administration and the Ministry of Science and Technology recently issued a roadmap setting up R&D priorities to boost science and technology innovation. Ocean engineering and "high-tech ships" are one of the ten strategic sectors of "Made in China 2025", the country's latest plan to lead globally on technological innovation. What is at stake for Europe is the long-term competitiveness of its own marine economy. This applies to competition on international export markets for ships, from naval systems to luxury cruise ships. Many analysts are dismissive of the current level of Chinese technologies, but this misses the upward trend and the political commitment of the Chinese leadership. As such, Chinese progress should be an incentive to consider policies that preserve the competitiveness of European industries.

Much of Europe's response – or lack thereof – to the Chinese naval buildup will depend on China's future clarification regarding its maritime strategy. But China did not need a sophisticated maritime strategy to invest massively in new capacities – the simple idea of wanting to become a major maritime power was sufficient. As this unfolds, the worst-case scenario for Europe is the emergence of a Chinese maritime strategy that relies too much on naval power, but does undermine the rules-based order, and shows little interest in international cooperation. After last year's South China Sea arbitration ruling, China has tended to see maritime law as a tool of the West, rather than a part of a rules-based order. China's decision to ignore the tribunal's ruling has created an uneasy status quo, exposing a new international division with regards to the universal value of the United Nations Convention on the Law of the Sea. Turning a blind eye on this division is not sustainable, as problems will resurface, and there is a risk that this divergence of interpretation evolves into a larger challenge against the rules-based order. Avoiding such an outcome has to be both the guiding principle for engagement with the PLAN and an element of Europe's thinking regarding its own naval capabilities.

NESI contributors and authors

Asli Aydintasbas – An expert on Turkey. Asli was formerly anchor at CNN Turk and Washington correspondent and later Ankara bureau chief for Sabah and columnist at *Milliyet*.

Julien Barnes-Dacey – An expert on Syria. Previously based in Damascus, Julien has worked as a journalist across the Middle East, reporting for the *Wall Street Journal*, the *Christian Science Monitor*, the *Financial Times*, Channel 4 News (UK) and Al-Jazeera.

Adam Baron – An expert on Yemen. Previously based Sanaa, Yemen, Adam worked as a journalist for a number of years.

Francisco de Borja Lasheras – An expert on Spanish foreign and security policy, the western Balkans, and nation building. Previously at the OSCE, Francisco spent several years in the Western Balkans, as Seconded National Expert to the OSCE Missions in Bosnia and Herzegovina.

Piotr Buras – An expert on the politics of European Union security. Piotr previously worked as Berlin correspondent for *Gazeta Wyborcza*.

Ruth Citrin – An expert on Syria and post-ISIS stabilisation. Ruth previously worked in the National Security Council in the White House, and in the US State Department.

Susi Dennison – An expert on migration. Susi was formerly an official in the British Treasury and with Amnesty International in Brussels.

Mathieu Duchâtel – An expert on Asian security, with a focus on maritime affairs, the Korean peninsula, China's foreign policy and EU-China relations. Mathieu is a former head of the SIPRI office in Beijing.

Anthony Dworkin – An expert on counterterrorism and international law. Anthony was previously with the Crimes of War Project and the BBC.

Sebastian Dullien – An expert on financial market regulation and economic warfare. He is a professor of international economics at HTW Berlin.

Silvia Francescon – An expert on global governance. Silvia is a former adviser to the prime minister and deputy head of the G8-G20 Sherpa office at the Italian Prime Minister's Office.

François Godement – An expert on Chinese and east Asian strategic and international affairs, regional integration, and conflicts. He is professor of political science at Sciences Po in Paris, and founder of and research associate at the Asia Centre.

Ulrike Esther Franke – An expert on emerging military technologies and German security policy. Ulrike is a scholar at Oxford University and was previously member of UN Special Rapporteur Ben Emmerson's research team on the use of drones for targeted killing.

Mark Galeotti – An expert on Russian intelligence and security. Mark is a professor of global affairs at New York University.

Ellie Geranmayeh – An expert on Iran. Ellie worked as a lawyer on public international law and sanctions regimes in London and Tokyo.

Richard Gowan – An expert on the United Nations, peacekeeping, and Africa. Richard is a fellow at the Centre on International Cooperation and formerly consultant to the UN Secretariat.

Gustav Gressel – An expert on the Russian military and an Austrian military officer, formerly with the Ministry of Defence.

Josef Janning – An expert on transatlantic relations, global governance and European security policy. Josef was previously director of studies at the European Policy Centre (EPC) in Brussels

Manuel Lafont Rapnouil – An expert on security crisis management and international security cooperation. Manuel is a former official at the French Ministry of Foreign Affairs.

Andrew Lebovich – An expert on north Africa and the Sahel. Andrew previously worked for the Open Society Initiative in west Africa and he has conducted field research Mali, Niger, and Senegal.

Mark Leonard – An expert on geopolitics and geo-economics. Mark is the co-founder of ECFR and most recently published "Connectivity Wars – Why migration, finance and trade are the geo-economic battlegrounds of the future".

Kadri Liik – An expert on Russia. Throughout the 1990s, Kadri worked as a journalist in Russia. She was the director of the International Centre for Defence Studies in Estonia.

Hugh Lovatt – An expert on the Israeli/Palestine conflict. He previously worked for the International Crisis Group and in the European Parliament.

Jeremy Shapiro – An expert on European counter-terrorism and military intervention. Jeremy is a former US State Department official and Brookings fellow.

Stefan Soesanto – An expert on digital issues and cyber, previously with RAND.

Angela Stanzel – An expert on Afghanistan and China. She has a *Ph.D* in Sinology, writing about China-Pakistan relations.

Vessela Tcherneva – An expert on the Balkans and European Union decision-making. She previously was the spokesperson for the Bulgarian Ministry of Foreign Affairs and secretary of the International Commission on the Balkans, chaired by former Italian prime minister Giuliano Amato.

Mattia Toaldo – An expert on Libya. Mattia is a member of the Council of the Society for Libyan Studies and has a *Ph.D* in the history of international relations.

Fredrik Wesslau – An expert on the Caucasus. Fredrik served as political adviser to the European Union Special Representative for the South Caucasus and for several years worked for the OSCE and United Nations in Kosovo.

Andrew Wilson – An expert on Ukraine and Belarus. Andrew is a professor in Ukrainian Studies at University College London.

Nick Witney – An expert on European defence and security. Nick was formerly chief executive of the European Defence Agency and an official at the British Ministry of Defence.

The tank icon used on the front of this publication is made by Freepik.

THE NEW EUROPEAN SECURITY INITIATIVE

"We live in a time of old conflicts and new threats in which the methods of warfare are changing. Europe needs to be at the forefront of security developments, lest it becomes the geopolitical plaything of others.

Not too long ago, Europeans thought they could project stability into their neighbourhood and make others more like them. But the Ukraine and Syria crises, the rise in domestic terrorism, and the use of cyberattacks forced it to rethink its position. A sense of urgency has to motivate member states to adapt to the new security environment.

In this collection ECFR's New European Security Initiative – NESI – deals with the new security environment Europe faces, looks at the capabilities Europe has and needs, and proposes how it can adapt before it is too late."

With contributions by:
Mathieu Duchâtel, Anthony Dworkin,
Ulrike Esther Franke, Gustav Gressel,
Mark Leonard, Manuel Lafont Rapnouil,
Stefan Soesanto, Mattia Toaldo,
and Nick Witney

EUROPEAN
COUNCIL
ON FOREIGN
RELATIONS
ecfr.eu

ECFR/222
ISBN 978-1-911544-22-7
9 781911 544227 >