Wilfried
Martens Centre
for European Studies

Dawn of the Drones

Europe's Security Response to the Cyber Age

Henna Hopia

Wilfried
Martens Centre
for European Studies

Dawn of the Drones

Europe's Security Response to the Cyber Age

Henna Hopia

Credits

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE 1000

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

For more information please visit:
www.martenscentre.eu

Editor: Benjamin Barth, Junior Research Officer, Martens Centre
External editing: Communicative English bvba
Layout and cover design: RARO S.L.
Typesetting: Victoria Agency
Printed in Belgium by Drukkerij Jo Vandenbulcke

This publication receives funding from the European Parliament.

Table of contents

Keywords Disruptive technology – Technological developments – Drones – Remotely piloted aircraft systems – Cyber attacks – Cyber defence – EU and NATO – European defence capabilities – Russia

About us

Martens Centre profile

The Wilfried Martens Centre for European Studies, established in 2007, is the political foundation and think tank of the European People's Party (EPP). The Martens Centre embodies a pan-European mindset, promoting Christian Democrat, conservative and like-minded political values. It serves as a framework for national political foundations linked to member parties of the EPP. It currently has 29 member foundations in 22 EU and non-EU countries. The Martens Centre takes part in the preparation of EPP programmes and policy documents. It organises seminars and training on EU policies and on the process of European integration.

The Martens Centre also contributes to formulating EU and national public policies. It produces research studies and books, electronic newsletters, policy briefs, and the twice-yearly European View journal. Its research activities are divided into six clusters: party structures and EU institutions, economic and social policies, EU foreign policy, environment and energy, values and religion, and new societal challenges. Through its papers, conferences, authors' dinners and website, the Martens Centre offers a platform for discussion among experts, politicians, policymakers and the European public.

About the author

About Henna Hopia

Henna Hopia is a foreign and security policy and EU specialist, freelance journalist and writer. She was a Visiting Fellow at the Centre for European Studies in 2012–13, during which time she wrote *Breaking Down the Walls: Improving EU–NATO Relations.* In Brussels she has worked as a correspondent for the newspaper *Nykypäivä,* in the European Parliament, and for a security and defence think tank. Prior to this, she worked for the Parliament of Finland, the Ministry of Defence of Finland and the National Coalition Party's Youth League.

Executive summary

This research paper examines two modern disruptive military technologies that are being used increasingly frequently: remotely piloted aircraft systems (RPAS) and cyber-attacks. These technologies are called disruptive because they are profoundly changing our societies and warfare. These changes also apply to Europe, so it needs to take them into account and adapt to the changes. More conventional threats have not disappeared, however, but are sometimes used alongside the new methods, as Russian aggression in Ukraine has shown. Europe is facing a hybrid threat with multiple elements that blend together and can change rapidly.

However, Europe is falling behind in developing or even dealing with new technologies. Insufficient investment has been made in research and development (R&D) and, due to a decline in military technology programmes, the European defence industry is suffering. If this continues we might lose important capabilities that have already been jeopardised by defence-budget cuts in recent years, and the existence of European military technology know-how could even be endangered. Creating European projects, such as a common RPAS, and economies of scale will be necessary to support the European defence industry.

Globally the number of countries and non-state actors possessing RPAS—including armed ones—has exploded. However, the EU is basically absent from this race. The EU needs to create common European requirements and pave the way for a European Medium Altitude, Long Endurance (MALE) RPAS, supported by NATO's expertise. RPAS have several advantages that should be appreciated, such as their cost-effective military value, ability to save human efforts and lives, and the spillover effects in the civilian domain, which offer remarkable potential for growth and jobs.

The tools to counter cyber hazards are also still deficient. Cyber-attacks pose an increasing and variegated threat to EU and NATO member states[1], which possess a high level of intellectual property and are dependent on the functioning of their critical infrastructure and information networks. The cyber dimension is a crucial element of Russia's new hybrid warfare and must therefore be taken into account even more vigorously. As NATO assessed at the Wales Summit in September 2014, cyber-attacks could reach a threshold that jeopardises national and Euro-Atlantic prosperity, security and stability. NATO, returning to its core duty of collective defence, is addressing the threat by including cyber-attacks under Article 5. The EU is mainly taking a civilian and legislative approach to cybersecurity, but is also promoting international norms that are

[1] In this research paper the term 'member states' can refer to both the EU member states and NATO nations.

still at a very early stage of development. The EU should, however, take cyber defence more seriously and better coordinate its cyber efforts. The work of the EU and NATO on cybersecurity is mostly complementary and could be further deepened. The matter of creating a credible cyber deterrent and suitable capabilities needs to be addressed.

The private sector is an important partner for both the EU and NATO. The concerns relating to drones and cybersecurity, such as the endangerment of privacy and unclear rules of engagement, have to be taken seriously. This approach will enable Europe to realise the full potential of these technologies while addressing concerns in society.

However, not everything can be done from Brussels; trust and the political will to invest in security have to come from the member states. Political parties can play a decisive role in generating this motivated atmosphere. Europeans are neither a risk to nor in competition with each other, but necessary companions in this ever-changing and insecure world.

Introduction

'If you want to build a ship, don't drum up the men to gather wood, divide the work, and give orders. Instead, teach them to yearn for the vast and endless sea.'

Antoine de Saint-Exupéry (1900–44), French writer and pioneering aviator

Technological developments have always had an impact on our societies, some more dramatic than others. When technologies change the system profoundly we can talk about disruptive technologies,[2] whose sudden dominance might come as a surprise to us.[3] What makes a technology 'game changing', 'revolutionary' or 'disruptive' is that it offers capabilities that were not previously available—ranging from the discovery of fire to the steam engine—and in so doing provokes deep questions which do not have answers at that time.[4]

Disruptive technologies can also have military applications—in fact their origin has often been in the military. In security, they can be defined as something that 'radically alters the symmetry of military power between competitors', 'immediately outdating the policies, doctrines and organizations of all actors.'[5] The history of mankind (which is largely also the history of war) has seen several of these disruptions, such as the inventions of gunpowder, aircraft, tanks, weapons of mass destruction and missiles. Contemporary disruptive military technologies include the remotely piloted aircraft systems (RPAS)[6] and other unmanned vehicles, robotics and autonomous systems, cyber technologies and data processing, the possibilities brought about by new materials to improve armour, and combinations of living and artificial organisms, amongst others.

[2] The term 'disruptive technology' was introduced by Harvard Business School professor Clayton M. Christensen in the mid-1990s. For more information see J. L. Bower and C. M. Christensen, 'Disruptive Technologies: Catching the Wave', *Harvard Business Review* (January/February 1995), 43-53; and C.M. Christensen, *The Innovator's Dilemma* (Cambridge, MA: Harvard Business School Press, 1997).

[3] N. Robinson et al., *Security Challenges to the Use and Deployment of Disruptive Technologies*, RAND Europe (Santa Monica, California, 2007), 7, 15.

[4] S. Brimley, B. FitzGerald and K. Sayler, *Game Changers. Disruptive Technology and U.S. Defense Strategy*, Center for a New American Security, Disruptive Defence Papers, September (Washington, DC, 2013), 4.

[5] Ibid., 11.

[6] There are several terms for these vehicles. In this research paper the term used is remotely piloted aircraft systems (RPAS), referring to the entity of the aircraft, the pilot and the command, while remotely piloted aircraft (RPA) refers to a single aircraft. Similarly well-known are the terms unmanned aerial vehicle (UAV), unmanned aerial system (UAS) and unmanned aircraft (UA). In spoken language, and also used in this paper, is the term 'drone', which originates from the first half of the twentieth century, when such objects were used as target practice and painted black and yellow for better visibility. For more information, see N. Wheeler, 'Remote Control: Remotely Piloted Air Systems', UK Parliament website, November 2013.

How, then, does this concern people who are not very technology-driven? These developments have an impact on all of us like never before. In addition to our civilian societies, the military is also more and more dependent on critical infrastructure such as functioning information networks. Military forces now widely recognise cyberspace as the fifth operational domain in addition to land, sea, air and space.[7] Traditional threats and challenges are being mixed with new elements and are changing fast. Instead of a pure cyberwar we are likely to see cyber-attacks[8] used as one tool in conflicts that have many other dimensions as well. In these 'hybrid wars', such as the war in Ukraine, the players are no longer just states but, for instance, covertly hired cyber hackers and unmarked troops. As a US Army study summarises: 'Defeating a hybrid threat, consisting of regular, irregular, and criminal elements synergistically working for a common end state, poses the greatest threat to the Army Profession of 2020 and beyond'.[9]

Moreover, high-level technologies had previously only been in the hands of a few states—this is about to change. By 2030 various non-state actors will increasingly be able to acquire technologies such as precision-strike capabilities, cyber instruments and bioterror weaponry, and 3D printing will enable anyone to produce weapons—reducing state control over the use of force.[10] On the international level, the West cannot expect to continue to have technological superiority, as a growing number of actors will have access to advanced military technologies. In fact, even now various countries and non-state groups possess armed drones. And as disruptive technologies alter the symmetry between opponents, small-sized actors, such as terrorist groups, could also become very powerful.

And as disruptive technologies alter the symmetry between opponents, small-sized actors, such as terrorist groups, could also become very powerful.

7 W. Röhrig and R. Smeaton, 'Cyber Security and Cyber Defence in the European Union, Opportunities, Synergies and Challenges', *Cyber Security Review* (Summer 2014), 24.

8 See various cyber-related definitions at NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 'Cyber Definitions'. As of yet there is no agreement on common 'cyber' terminology either internationally or even on the European level. Some Oxford definitions of terms used in this paper: cyber—'relating to or characteristic of the culture of computers, information technology, and virtual reality'; cybersecurity—'the state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this'; cyber threat—'the possibility of a malicious attempt to damage or disrupt a computer network or system'; cyber-attack—'an attempt by hackers to damage or destroy a computer network or system'; cyberwar—'the use of computer technology to disrupt the activities of a state or organisation, especially the deliberate attacking of communication systems by another state or organisation'; cyberspace—'the notional environment in which communication over computer networks occurs'.

9 J. R. Davis, Jr., 'U.S. Army, Defeating Future Hybrid Threats. The Greatest Challenge to the Army Profession of 2020 and Beyond', *Military Review* (September/October 2013), 21.

10 G. Grevi, et al., *Empowering Europe's Future: Governance, Power and Options for the EU in a Changing World* (European Union, 2013), 11.

There is grave concern over how Europe will cope with these developments, especially as EU countries have downsized their defence budgets during the last decade and crucial investments in R&D have not been made, leaving us vulnerable. The EU and NATO have recently stepped up their efforts, but is that enough?

This research paper examines the current state of affairs in Europe when it comes to RPAS and cyber-attacks, as they are the disruptive technologies currently most clearly on the political and institutional agenda in Europe; in December 2013 the European Council made a concrete decision on them, and NATO also sees critical shortfalls in these capabilities.[11] The questions the author addresses are: where does Europe—the EU and also NATO—stand on these issues politically and legislatively? What are the threats, challenges, dilemmas and opportunities?

This research paper first looks at the case of RPAS, describing the current situation, European efforts and also the lack of them, and analyses the moral and international debate over drones. The second part focuses on cyber-attacks; the different kinds of threats and responses from the national, EU and NATO levels; and internal and international cyber issues. The third part will combine the two elements by introducing conclusions and policy recommendations for a way forward.

[11] Interview with a NATO military officer on 13 June 2014.

Drones: debatable but indispensable devices

The European drone

Everybody wants one

RPAS have been a growing trend in aviation for several decades, but it is only in recent years that their ownership has exploded: currently over 70 countries possess RPAS, over 50 with their own programmes, of which 23 have armed programmes.[12] China, India, Iran, Russia, Taiwan, Turkey, the United Arab Emirates and the US are all developing Medium Altitude, Long Endurance (MALE) drones that can be used for intelligence gathering, surveillance, target acquisition, reconnaissance and attack.[13]

However, Europe still does not have a drone that is capable of combat operations. The EU uses surveillance drones in its missions but it does not have enough of them—this was made clear in Mali and Libya when Europeans had to rely on American drones. It is through these experiences that the need to establish European drone capabilities—as well as cyber and air-to-air refuelling capabilities—has become clear.

There are several ongoing European projects, most of them led by Europe's top defence spenders, France and the UK. For instance, Dassault Aviation and BAE Systems are working together on Telemos, a MALE drone. The Germans and Spaniards are developing Barracuda, and the French are leading a six-country endeavour (alongside Sweden, Greece, Italy, Spain and Switzerland) to create the nEUROn, an experimental Unmanned Combat Air Vehicle that has already flown in formation with manned aircraft.

EU: licence to drone

For the EU to be a serious actor in security and foreign policy and carry out successful operations, a European drone is seen as a strategically important endeavour. It is also such an expensive initiative that

[12] L. E. Davis et al., *Armed and Dangerous? UAVs and U.S. Security*, RAND Corporation (Santa Monica, California, 2014), 9.
[13] Ibid.

cooperation at the bilateral or intergovernmental level is not sufficient; only an EU-level approach will work.[14] Such an endeavour would also reduce Europe's dependency on US technology. According to Airbus Military's managing director, 'European nations must unite around a single drone capable of combat operations if it is to catch up with the US in unmanned aircraft technology.'[15] The EU has recently taken some very visible steps to improve the legislative framework in order to enable this European project, having already undertaken several years of preparatory work on the technological requirements. In recent years the Commission has introduced legislation to strengthen the European defence technological and industrial base,[16] and the EU High Representative for Foreign Affairs and Security Policy presented propositions to enhance EU defence capabilities in the run-up to the European Council on defence in December 2013.[17] The European Council endorsed the plans to create a European MALE drone by 2020–5 [18] following a Letter of Intent from seven EU member states (France, Germany, Greece, Spain, Italy, the Netherlands and Poland) declaring their intention to create a European MALE RPAS community.

When aerial legislation was drafted it only took into account manned aircraft, so it is not easy to introduce RPAS into civilian-controlled airspace; the European Commission, the Single European Sky Air Traffic Management Research Joint Undertaking and Eurocontrol are working on this extensively. Europe's densely populated airspace complicates the task, and both civilian and military RPAS will have to comply with civilian regulations (whereas in Israel, for instance, most of the airspace is under military control and drones can fly around more freely).[19]

---

[14] Interview with an assistant to a European People's Party (EPP) Member of the European Parliament (MEP) on 13 May 2014.

[15] M. Stothard and A. Parker, 'Airbus Chief Calls for United EU Drone Project', *Financial Times*, 16 July 2014.

[16] See, for instance, European Commission, *A New Deal for European Defence, Towards a More Competitive and Efficient Defence and Security Sector*, Communication, COM (2013) 542 final (24 June 2014); and European Commission, *Towards a More Competitive and Efficient Defence and Security Sector,* Communication, COM (2013) 542 final (24 July 2013), which build on European Parliament and Council Directive 2009/81/EC on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC (Text with EEA relevance), OJ 216 (13 July 2009), 76; and European Parliament and Council Directive 2009/43/EC simplifying terms and conditions of transfers of defence-related products within the Community (Text with EEA relevance), OJ L146 (6 May 2009), 1. Also, in 2011 the Commission's Directorate-General Enterprise and Industry and Directorate-General Internal Market and Services jointly established a Commission Task Force on the Defence Industry and Markets.

[17] EEAS, *Preparing the December 2013 European Council on Security and Defence*, *Final Report by the High Representative/Head of the European Defence Agency (EDA) on the Common Security and Defence Policy* (Brussels, 15 October 2013).

[18] European Council, *Conclusions*, EUCO 217/13 (20 December 2013).

[19] Interview with a European Commission official on 27 May 2014.

The Commission introduced a Communication on civil drones in April 2014, with the aim being for civil RPAS to fly in civil airspace from 2016 onwards.[20] The need for RPAS airspace integration is urgent for both safety and business reasons and requires increased coordination.[21] The Communication calls for the development of EU-wide safety standards for civil RPAS by the European Aviation Safety Agency. This requires in particular the harmonisation of national requirements and standards for light (< 150 kg) civil drones. The development of safety standards for civil drones benefits military projects as they could contribute to military certification. On its side the European Defence Agency (EDA) is working on the harmonisation of military requirements for MALE RPAS. This is important as one problem with the European MALE RPAS project is the existence of different national standards and requirements.

The ideal situation would be for the European MALE drone to be EU owned and able to be used for both civilian and military purposes with Frontex and for Common Security and Defence Policy (CSDP) missions abroad.[22] It is too early to estimate what reality will look like for the European drone—how will the EU framework be incorporated? Will the capability be shared between the seven participating nations? Will there be one fleet, following the example of air-to air-refuelling, or is RPAS too sensitive a capability for that?[23] There is still not enough trust between the member states. Even if the EU was to be given 'a licence to drone' and a European MALE was introduced, there are still many questions that need to be answered, and the whole process could take a long time. With the Airbus A400M transport aircraft this process took over a decade.

The need for RPAS airspace integration is urgent for both safety and business reasons and requires increased coordination.

EU equals European; NATO equals American?

NATO also has a project to develop a High Altitude, Long Endurance (HALE) drone; however, the aircraft is not European. The operation in Libya in 2011 exposed NATO's shortfalls in intelligence, surveillance and

[20] European Commission, 'European Commission Calls for Tough Standards to Regulate Civil Drones', Press Release (8 April 2014).
[21] J. P. Lentz, 'A Roadmap for RPAS Integration in European Airspace by 2016', presentation at the European Commission Directorate-General Enterprise and Industry ASD Convention Technology Forum, Lisbon, 11 October 2012.
[22] Interview with an assistant to an EPP MEP on 13 May 2014.
[23] Interview on 6 June 2014 with a journalist who specialises in defence matters.

reconnaissance capabilities, and the Alliance signed up for a procurement contract for the Alliance Ground Surveillance System in May 2012 at the NATO summit in Chicago. About half of the Allies are involved in this project. The system will be owned by NATO and available for all Allies from 2017 onwards. It can be used for widely varying missions, such as force protection, crisis management, peace support, border and maritime security, and humanitarian assistance. The drones that NATO has acquired are five unarmed Global Hawk drones from the American Northrop Grumman group,[24] therefore continuing the tradition of relying on American capabilities. Procuring from outside Europe has not been without problems, as Germany's experience with the Euro Hawks shows. This order from Northrop Grumman had to be cancelled as the Americans did not provide all the technology needed for the device to fly in European airspace.

Indeed not all are demanding the creation of a European drone. In an interview one national military officer admitted that in the end it is merely a political decision as to whether the EU acquires an RPAS or not: 'I don't care where the capability comes from, as long as it comes.'[25] But as the political decision has been made on the European drone project, it is clear that it will be carried out in the EU context; there are no industrial projects within NATO and the aviation sector is controlled by civil authorities.[26]

However, NATO also has a role in the EU's MALE RPAS project. NATO is defining the standardisation agreements to increase interoperability in order for the European MALE to be built according to NATO standards.[27] Naturally this is beneficial, as it paves the way for improved cooperation between the two organisations. In addition, use of the NATO platform will ensure the interoperability of RPAS vis-à-vis other military forces, such as ground stations and satellites. NATO has also included RPAS as a major element in its exercises, thus delivering its experience to the EU via the joint member states.[28] And should the Berlin Plus agreement one day become operational again, maybe the EU could borrow the NATO HALE capability when needed, to complement the MALE fleet?

---

[24] NATO, 'NATO Alliance Ground Surveillance Programme takes off in Chicago', Press Release, 21 May 2012; and NATO, 'Alliance Ground Surveillance (AGS)', Fact Sheet, 16 May 2012.

[25] Interview with a national military officer on 22 August 2014.

[26] Interview on 6 June 2014 with a journalist who specialises in defence matters.

[27] Ibid.

[28] Ibid.

Europe has missed a step

Weak investments, weak industry

The setting for European capabilities is challenging, as investments in defence have not been made. The Americans and Israelis are far ahead of Europe, both in military and dual-use (for both civilian and military purposes) technologies. China and other nations are eclipsing Europe quickly—'in some technologies we are still ahead of them thanks to investments we made 20 years ago . . . but in four to five years, they will surpass us. From a technological point of view, Europe has missed one step of development.'[29]

The European defence market has remained fragmented due to nationally defined demand, supply and regulations, and also due to Article 346 of the Treaty on the Functioning of the European Union that exempts the application of EU rules on procurement for reasons of national security, which can be used for protectionist purposes.[30] In addition to fragmentation there is also obvious overcapacity, for instance in the defence ship-building and land-armament sectors.[31] 'Why do we have tanks in excess but have to borrow RPAS from the Americans?' questioned one European Commission official in an interview.[32] These defects have prevented European companies from reaching economies of scale and financial critical masses, unlike their counterparts in the US.[33]

A European MALE would not be a miracle in terms of saving the industry, but it would be a start, and there does not seem to be much of a choice: one interviewee believes that 'Either we go for a European approach on major defence programmes or we will not have a European defence industry any more.'[34]

---

29 Interview with a European Commission official on 27 May 2014.

30 A. Frontini, 'Beyond the "Guns or Butter" Dilemma – The December European Council and the Future of the European Defence Industry', European Policy Centre, Commentary (Brussels, 4 December 2013).

31 A. Missirolli (ed.), *Enabling the Future – European Military Capabilities 2013-2025: Challenges and Avenues, EU Institute for Security Studies* (Paris, 2013), 10–11.

32 Interview with a European Commission official on 27 May 2014.

33 Frontini, 'Beyond the "Guns or Butter" Dilemma'.

34 Interview on 6 June 2014 with a journalist who specialises in defence matters.

The European drone might even offer a breakthrough, as the authors of one policy brief hope: 'If Airbus became a global leader, so the RPAS initiative can produce a global player.'[35]

Because of the decline in military technology programmes the European defence industry is suffering. The intended merger of EADS and BAE Systems in 2012 would have stimulated the industry, but the German withdrawal caused the deal to fall apart. And even though European countries have competing armament programmes, according to one European study there is little research happening on future capabilities such as fifth- and sixth-generation aircraft.[36] The medium- and long-term defence-related investment programmes are being implemented by and through different bodies in the Commission and the EDA, which adds to the segmentation: programmes are dealt with in separate places with their own procedures, with each having something of a military dimension, but none exclusively so.[37]

From dual-use to defence funding?

Without military programmes, defence companies are increasingly focusing on the civilian side and risk losing their military expertise.[38] The Commission is encouraging the industry to seek research funding where it can. EU research funds under the Horizon 2020 programme[39] have been strictly allocated for non-military purposes—something that many MEPs and some member states are insisting on, even though Article 45 of the Lisbon Treaty clearly says that defence research has to be funded by the EU.[40] However, Horizon 2020 does allow dual-use research funding and this is now being used to compensate for the lack of defence research. This is useful because military technology is increasingly dependent on developments in the civilian world and the key enabling technologies can be used for both military and civilian applications. In the future there is some hope for Common Security and Defence Policy (CSDP) related research

[35] J. Coelmont and S. Biscop, *Building European Defence: An Architect and a Bank*, Security Policy Brief no. 56, Egmont Royal Institute for International Relations (Brussels, May 2014), 2.
[36] Missirolli (ed.), *Enabling the Future*, 10–11.
[37] Ibid., 13.
[38] Interview with a European Commission official on 27 May 2014.
[39] Horizon 2020 is the EU Framework Programme for Research and Innovation for the years 2014–20 with funding totalling nearly €80 billion. For more information, see http://ec.europa.eu/programmes/horizon2020/.
[40] Interview with a European Parliament official on 22 May 2014.

funding as the Commission has proposed a Preparatory Action which, if successful, means a CSDP component could be added to the next Multiannual Financial Framework research programme.[41]

Important R&D thresholds have also not been met: regardless of their own commitments to allocate a minimum of 2% of their defence expenditure on R&D, at least until 2010 five member states had spent zero, and only one country (Sweden) had reached the objective.[42] The member states themselves decide what projects to fund, for instance RPAS; at the moment there is not even a budget for the dual-use aspect of RPAS.[43]

Also, the EDA's budget and role have been kept to a minimum. Regarding RPAS, the EDA declares that its objective is to 'exchange information and identify and facilitate cooperation among member states that currently operate or plan to operate RPAS'.[44] Some argue that the EDA could have a much larger role as a coordinator of the drone programme throughout its life cycle, offering a dissemination mechanism and discussion platform, and ensuring cost-effectiveness and interoperability. Some policy researchers believe that the EDA could offer a channel to the Commission, which could participate in the programme's funding as does a member state, and also to the European Investment Bank, which could function as the bank for the member states' financing of projects.[45] However, this seems unrealistic as the EDA's hands are tied, with the member states holding the power and the Commission holding the funding. For example, developing technologies to ensure safe flights is important both for military and civil drones and most of them are of dual-use nature. As the Commission cannot fund military projects it looks for strong coordination with EDA dual-use projects in this area.[46]

[...] the EDA's hands are tied, with the member states holding the power and the Commission holding the funding.

According to one journalist who closely follows developments in the defence sector, the dual-use potential will be used to its fullest, stretching the definition: 'They won't be able to procure weaponry but all the

41 Interview with a European Commission official on 27 May 2014.
42 European Parliament, *Resolution on Cyber Security and Defence*, 2012/2096(INI) (22 November 2012), 7.
43 International Security Information Service Europe, 'Parliamentary Update no. 56, SEDE Subcommittee', 12 February 2014.
44 EDA, 'Defence Ministers Commit to Capability Programmes', Press Release (19 November 2013).
45 Coelmont and Biscop, *Building European Defence*, 2–3.
46 Interview with a European Commission official on 27 May 2014.

support systems for weaponry, such as communications, intelligence and RPAS, they will.[47] The journalist believes that the Commission will also get its share of defence funding in the upcoming years, even though it will most likely not actually be called this.[48] It is up to the decision-makers to determine whether this will be made possible, or whether Europe will miss steps in the future as well. Also, from the point of view of legitimacy, it would be only reasonable to expect that this would be done in a transparent fashion.

Bad reputation, but badly needed

RPAS have existed for decades but as technology has advanced—with GPS, design, armaments and technological gadgets—in recent years they have become unbeatable in many ways and their use has become less exceptional. RPAS have diverse functions and can be a great asset in military and especially civilian applications. Many of their advantages are widely recognised, but concerns relating to their use have undermined their proper launch in Europe. The concerns are genuine and should be discussed openly and rules adapted accordingly; fear and prejudices can be overcome. To tackle this, a list of advantages and concerns relating to RPAS follows.

Advantages and strengths

- RPAS have proven their military value by demonstrating their operational capacities, particularly in surveillance and information gathering.[49] Reconnaissance drones are very useful in crisis management operations, as shown by the UN missions in Mali and the Democratic Republic of the Congo. Drone technology was also used widely in Afghanistan during the NATO operation. Currently the Organization for Security and Co-operation in Europe is using monitoring drones in Eastern Ukraine.

47 Interview on 6 June 2014 with a journalist who specialises in defence matters.
48 Ibid.
49 EDA, 'Defence Ministers Commit'.

• There is a demand for RPAS in contemporary military operations, for instance British Defence Secretary Michael Fallon sees Reapers as providing 'vital situational awareness', making them an 'invaluable asset'.[50] Indeed, the UK is deploying armed Reaper drones in Iraq to fight Islamic State militants. One indicator of RPASs' attractiveness might also be that the US Air Force is now training more RPA pilots than pilots for manned aircraft. Drones can also be very useful in post-operation situations; as the main troops leave Afghanistan the use of drones should greatly reduce the risk of the country becoming a safe-haven for terrorists.[51]

• RPAS are quickly deployable, can fly for longer than manned aircraft and can engage in combat repeatedly. They are quite cheap to produce and manage as the vehicles do not have to include the room and safety equipment required for a pilot (less fuel, no life-support systems and lower personnel costs).

• In military missions they diminish the amount of own-side casualties; there is no fear of losing the pilot, be it in an armed operation or a dangerous surveillance or rescue mission, which might make the decision to carry out or participate in a necessary mission easier. Also, the likelihood of collateral damage is lowered as 'the probability of mistakes and unintended attacks (with RPAS) is significantly reduced compared to engagements from manned aircraft', due to their increased operational and tactical-level interfaces.[52] RPAS offer more control than a manned aircraft, provide a good look at the terrain and are precise. For instance, their cameras are rapidly evolving to further reduce the possibility of error; the latest cameras allow the pilot to zoom in extremely close, without losing the broader view of the terrain.

The concerns [about RPAS] are genuine and should be discussed openly and rules adapted accordingly; fear and prejudices can be overcome.

• RPAS can be very useful tools for police, border control and other state authorities besides the military. They are especially suitable in operations where a pilot would only be at a disadvantage or his life endangered, such as in fire fighting, dealing with natural disasters, radiation monitoring and pest control.

[50] Reuters, 'Armed UK Drones Deployed in Iraq, Support Fight against ISIS', 16 October 2014.
[51] D. Byman, 'Why Drones Work. The Case for Washington's Weapon of Choice', *Foreign Affairs,* July/August 2013.
[52] Joint Air Power Competence Centre, *Remotely Piloted Aircraft Systems in Contested Environments: A Vulnerability Analysis* (Kalkar, September 2014), 51.

They are very useful in long-enduring tasks, such as surveillance missions or search and rescue, where a single pilot flying a plane would eventually tire.

• The technology can offer many solutions for different kinds of needs. For instance, the EU's border control agency Frontex is keen to use 'optionally piloted aircrafts' that can either carry a pilot or be used unmanned, depending on the nature of the mission.

• RPAS offer huge potential for civilian functions, where they are increasingly being used. Opportunities exist, for instance, in aerial photography and digital mapping, measuring air quality, agriculture and forestry, inspections of power lines and oil and gas pipes, monitoring of road security, logistics, and everyday consumer services such as the home delivery of goods. The civil applications for small and medium-sized enterprises offer a lot of potential for growth and jobs: it is estimated that in the next decade the RPAS business could be worth 10% of the aviation market, €15 billion per year.[53] RPAS represent 'a revolution in technology in much the same way the aircraft itself was', noted the chair of the EU Military Committee.[54] This technology will lead to another revolution in civil aviation with, as a minimum, cargo planes flying without pilots, which would mean cuts in costs and more efficient transport.

Concerns and fears

Military drone operations being carried out outside of internationally recognised zones of armed conflict.

This is one of the most debated issues, due to US Central Intelligence Agency covert counter-terrorism operations in Pakistan, Yemen and Somalia. European RPAS endeavours have been somewhat affected by this discussion, which has also been prominent in debates in the European Parliament (EP).[55] MEPs were unanimous on the requirement that the EU would have to commit to only operating armed drones in recognised warzones. The EU should commit to this and promote this policy in international fora.

[53] European Commission, 'European Commission Calls for Tough Standards'.
[54] International Security Information Service Europe, 'Parliamentary Update no. 56'.
[55] European Parliament, *Joint Motion for a Resolution on the Use of Armed Drones*, 2014/2567(RSP) (25 February 2014).

Concerns about secrecy.

The Central Intelligence Agency's operations have created concerns about the lack of transparency in operations and the victims' identities. It is clear that Europe has to be transparent and open and promote this approach internationally.

Civilian casualties.

This concern is closely related to the first two. If operations are legal and transparent, the number of civilian casualties is likely to be lower. Civilian casualties are always a tragedy; unfortunately they can befall any operation, whether using manned or unmanned vehicles. As stated above, however, target accuracy with drones is better than with manned aircraft. If there are errors, it is often the intelligence that needs to be more precise. The problem of what to do with the wounded or prisoners of war is another valid concern,[56] but this also exists with fighter jets. The way to reduce the impact of this is to be more transparent and open when it comes to collateral damage; secrecy only makes matters worse.

The claim that RPAS are 'less human' than manned armed aircraft.

It is argued that due to the distance of the operators from the warzone, and because the operators are not putting themselves in the line of fire, they lose their human sensibilities and the threshold for firing might be lowered. But what really is the difference between pulling the trigger of a rifle, launching a missile or firing an armed drone? The type of weapon or distance plays no part here: there is and should always be a chain of command, leading to the political top, and we need to be able to trust that these decisions are not taken lightly. RPAS are no less 'human' than any other device that can be used as a weapon—it is about how and on what principles the devices are used.

[56] Interview with an EP official on 22 May 2014.

Concern that drone strikes create radicalisation in the target population.

International law should be respected when carrying out operations. It is obvious that grey areas will remain a challenge, but maximum effort should be made to address all concerns regarding legality and legitimacy. Terrorists using humans as shields is a concrete example of one such complex situation.

Privacy.

There will be more and more drones in the hands of citizens who might misuse them, so law enforcement agencies need drones to ensure public security. However, as RPAS, like any other technological device today, gather information, data privacy is an important issue. Through legislation and political control the risk of misusing the information gathered can be diminished; guidelines, for instance, on how law enforcement agencies may use information gathered by RPAS need to be clear. Alongside the privacy issue, the European Commission acknowledges that the other societal impacts of RPAS need to be addressed, such as liability, insurance, protection and public acceptance.[57]

The vulnerabilities of RPAS.

One concern is that RPAS are vulnerable to cyber-attacks, and that they might even be electronically hijacked. Consequently more attention needs to be paid to better cyber protection. Drones require clear airspace in which to operate and would not be efficient against enemies such as Iran or North Korea. Also, important intelligence information might not be acquired if there are no prisoners to interrogate. RPAs are also very easy to shoot down;[58] however, any aircraft can be shot down, and in this case there would be no casualties. A recent NATO study warns of the possibility of enemies attacking RPAS operators,[59] but if there is enough distance and sufficient classification of the location of troops then this risk can be reduced significantly.

---

[57] Lentz, 'A Roadmap for RPAS Integration'.
[58] A. K. Cronin, 'Why Drones Fail. When Tactics Drive Strategy', *Foreign Affairs*, July/August 2013.
[59] Joint Air Power Competence Centre, *Remotely Piloted Aircraft Systems in Contested Environments*, 51.

Proliferation.

Armed RPAS are also increasingly falling into the hands of non-state groups and terrorists. Little can be done to stop proliferation as RPAS are easy to produce. Drones are also very suitable for delivering biological and chemical weapons. Hence it is important to prepare for threat scenarios where the adversary is in possession of this technology, and it is even more important to promote a clear set of international rules, as the current vague setting and precedent set by the US might be used as an excuse for others to start targeted killing campaigns to suit their own purposes, even against their own people.

An aircraft flying without a pilot is a concept that might cause us fear.

According to one expert, however, 'the biggest cause of accidents nowadays is human error'.[60] Cargo is already being transferred without pilots, and trains are travelling without drivers—and autonomously, without even remote control from a human. Regardless, this is an issue that should not be overlooked: the technology has to be reliable, there must be human supervision and safety precautions must be put in place, including strict emergency procedures. Also, as MEPs have demanded,[61] there must always be 'a human in the loop', a human being in charge when firing an armed drone.[62] This is an issue where more debate is expected as the technology is becoming increasingly autonomous. The US Air Force predicts that 'the use of autonomous systems will be the single most significant feature of military technology in the coming decades'.[63]

---

60 Interview with a European Commission official on 27 May 2014.
61 European Parliament, *Joint Motion*.
62 Interview with an assistant to an EPP MEP on 13 May 2014.
63 G. Grevi et al., *Empowering Europe's Future,* 39-40.

Learning from the past

As listed above, many concerns are derived from the US use of drones in targeted killings in non-belligerent states which, according to international humanitarian law, is illegal. This has understandably brought about a moral discussion on the use of armed drones and the secrecy of these operations. But the issue is not black and white. The effectiveness of these counterterrorism operations should not be undermined; for instance in Pakistan during the past decade drone strikes have cut the number of core al Qaeda members in tribal areas by about 75%, and in general the drone threat has hindered terrorists from operating as they normally would.[64] The critics of drone strikes often fail to take into account that the alternatives to the use of drones to hunt down terrorists in remote and hostile territories are 'either too risky or unrealistic'.[65] It is not always wise or possible to declare a war on the country where terrorists are hiding. It is also worth remembering that in some cases, such as in Pakistan, the national government supports the US strikes. It is also not very clear whether the estimates of the numbers of civilian casualties and the reported lack of local support for US drone operations are correct.[66]

The American experiences should not turn Europe away from drones, but rather be used to learn how to use the devices as responsibly as possible.

Regardless of this and the successful anti-terrorism operations, there is a risk that the overall war might still be lost. US strikes and civilian casualties—and especially the secrecy surrounding them—might help al Qaeda in its recruitment and propaganda, even though it is al Qaeda that aims to cause civilian casualties and not the US.[67]

The American experiences should not turn Europe away from drones, but rather be used to learn how to use the devices as responsibly as possible. Ultimately, when it comes to moral questions, RPAS do not really differ from manned aircraft or helicopters, or other similar weapons, which can all be used in both a right and a wrong way. Therefore Europe has to have a strategic and long-term vision to its approach, and this can only be achieved by basing its actions on a clear, values-based legal framework.

64 Cronin, 'Why Drones Fail'.
65 Byman, 'Why Drones Work'.
66 Ibid.
67 Cronin, 'Why Drones Fail'.

The resolution from the EP on armed drones can be used as a starting point: it bans extrajudicial targeted killings and fully autonomous weapons, and includes armed drones in the relevant European and international arms control regimes.[68] There needs to be more transparency and accountability when it comes to using armed drones, and member states need to adopt a common position on them.[69] Armed drones should only be used after considering the potential gains and risks, and in situations where they advance the overall strategy. In general, the international framework concerning engaging in war (*jus ad bellum*) and waging war *(jus in bello)* should be clarified. Having a clear set of international rules would also preclude any other state which might now take advantage of the current ambiguous setting from conducting targeted killings in an unlawful or immoral manner.

[68] European Parliament, *Joint Motion*, 4.
[69] Ibid., 4.

Cyber-attacks: complex and camouflaged

A multifaceted threat

How, why and who?

Technology can be used to our advantage, but also against us. When asking how serious a threat cyber-attacks can be, one gets several responses, as they pose a different level of risk to different states. A clear correlation between technological advancement and vulnerability exists: for European countries with large industries and a lot of intellectual property, cyber-attacks are a serious menace.[70] At the Wales Summit in September 2014 NATO acknowledged that cyber-attacks 'can threaten national and Euro-Atlantic prosperity, security, and stability'; 'will continue to become more common, sophisticated, and potentially damaging'; and that 'the impact of cyber attacks could be as harmful to modern societies as a conventional attack'.[71]

There are several motivators to conduct cyber-attacks—to steal money, to conduct industrial espionage, or to use the information gathered for political and military purposes. A recent study describes cybercrime as 'a growth industry, where returns are great, and the risks are low'.[72] The study estimates that governments and companies underestimate the cyber risk, which costs the global economy about €300–400 billion annually.

A military expert and McAfee Cybersecurity Director Jarno Limnéll describes three levels of cyber-attack: first, 'business as usual', which means service denial such as website disruptions (usually outsourced to 'hacktivists'); second, information operations, in other words propaganda and disinformation; and third, and most severe, attacks on critical infrastructure.[73] Cyber-attacks on critical infrastructure—energy, communications, logistics, financial institutions and governance—are estimated to be the most damaging that

[70] Interview with a NATO official on 25 June 2014.
[71] NATO, 'Wales Summit Declaration', Press Release, 5 September 2014.
[72] Intel Security, *Net Losses - Estimation the Global Cost of Cybercrime*, *Economic Impact of Cybercrime II* (Santa Clara, California, June 2014), 2.
[73] J. Limnéll, 'Ukraine Crisis Proves Cyber Conflict is a Reality of Modern Warfare', *The Telegraph*, 19 April 2014.

this sort of threat can impose on us.[74] Attacking critical infrastructure might also only be a first step; after neutralising infrastructure and creating chaos the perpetrator might then physically attack the country.[75]

Cyber-attackers range from individual hackers to organised crime groups and states. States can also use individuals and groups to do the dirty work on their behalf in order to remain camouflaged themselves. All major powers are thought to have used cyber capabilities as a political and even military tool. For instance, it is believed that the US and Israel introduced the Stuxnet malware into Iranian nuclear centrifuges in 2010.

Even though it is difficult to attribute attacks to certain countries as they leave no physical evidence behind, aggregate data (time zone, location of the attacking servers, nation-specific tools and techniques, and language indicators) have led researchers to place the majority of the blame on Russia and China.[76]

It is estimated that there are 20 to 30 cybercrime groups in the former Soviet Union that have 'nation-state level' cyber capacity and can overcome even highly sophisticated cyber defences.[77] 'All the Russian-speaking countries are territories where the EU companies receive serious cybercrime activities', one European External Action Service (EEAS) official observed in an interview.[78] China tops the statistics for cyber-attacks for espionage and financial gains as the country of origin for 41% of attacks.[79] China is believed to steal intellectual property from the US on a regular basis. According to the US government, China is using its advanced cyber capabilities to conduct large-scale cyber operations that target, for example, the networks of the US Department of Defense and defence contractors, 'posing a major threat' to American military operations, personnel, effectiveness and readiness.[80]

For European countries with large industries and a lot of intellectual property, cyber-attacks are a serious menace.

[74] Interview with a NATO official on 25 June 2014.
[75] Interview with an EEAS official on 6 June 2014.
[76] D. J. Summers, 'Fighting in the Cyber Trenches', *Fortune*, 13 October 2014.
[77] Intel Security, *Net Losses - Estimating the Global Cost of Cybercrime,* 15.
[78] Interview with an EEAS official on 13 June 2014.
[79] See, for instance, Akamai Technologies, *Akamai's State of the Internet, Q1 2014 Report*, vol. 7, no. 1 (2014).
[80] L. M. Wortzel, *'Cyber Espionage and the Theft of U.S. Intellectual Property and Technology', Testimony of Larry M. Wortzel before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations,* Summary of Testimony (Washington, DC, 9 July 2013), 3–4.

As an example of the results of such espionage, the Chinese J-31 stealth fighter is believed to be based on American F-35 technology.[81]

Russia, Russia, Russia

Russia is well-known for using cyber methods for political and military purposes, and for hiring Internet trolls to carry out attacks, propaganda and disinformation. For instance, according to one security analyst, 'Russian state-backed cyber spies are behind co-ordinated, sophisticated digital attacks in the past two years against sensitive political and military targets, including NATO, the EU and government ministries'.[82] European diplomats have become targets in a growing number of attacks, and of extensive and sophisticated cyber espionage campaigns as the war in Ukraine has escalated. During the so-called referendum in Crimea in March 2014, NATO was the target of several cyber-attacks.[83]

Cyberwar is an integral part of Russia's hybrid warfare strategy—this is a situation the West should take seriously. In the Institute de Recherche Stratégique de l'Ecole Militaire's publication of December 2014, the editor explains that hybrid wars are not new as a concept in the literature of war studies, but what is striking now is the connection between the obscurity of war and the obscurity of the participating states' decision-making. The multiplicity of actors and situational logics escape even the capacities of the resourceful states involved, especially since states' actions and decisions are extremely difficult to identify from the outside.[84] In the same publication a researcher writes that NATO should deter and respond 'to potential contingencies, including the "hybrid warfare" practiced by Russia against Ukraine.'[85] Another author writes that NATO 'has not yet found an answer to the new sort of "hybrid threats", when non-military elements of cyber war, propaganda, informal fighters and energy dependence play important

[81] Ibid, 5.

[82] S. Jones, 'Russian Government Behind Cyber Attacks, Says Security Group', *Financial Times*, 28 October 2014.

[83] S. Jones, 'Nato Summit on "High Alert" for Cyber Attack', *Financial Times*, 3 September 2014; A. Croft and P. Apps, 'NATO Websites Hit in Cyber Attack Linked to Crimea Tension', *Reuters*, 16 March 2014; and S. Jones, 'Ukraine PM's Office Hit by Cyber Attack Linked to Russia', *Financial Times*, 7 August 2014.

[84] F. Charillon, 'Guerres hybrides et processus décisionnels incertains', Editorial, *La lettre de l'IRSEM* 8, 19 December 2014, 1-2.

[85] L. Michel, 'An American Perspective on the Wales Summit: Now Comes the Hard Part', *La lettre de l'IRSEM* 8, 19 December 2014, 9-10.

roles in overall strategy.' He adds, 'Now, no war has ever been only fought by the military, but Russia has perfected the strategic use of non-military pressure.'86

Russian cyber-attacks during the war in Ukraine did not come as a surprise, as massive cyber-attacks had been carried out against Georgian websites and financial systems prior to Russia's tanks rolling into the country in 2008. The Russian cyber-attacks on Estonian government websites, banks and the media in summer 2007, following a dispute over the relocation of the Bronze Soldier (a Russian symbol of its victory over the fascists in the Second World War but a reminder for Estonians of Soviet occupation) acted as a wake-up call for Europe. In fact, Russia spurred NATO to step up its cyber defence efforts, basically chose the location for the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)—Tallinn—and inspired Estonia to become one of the countries with the best cyber know-how.

Limnéll argues that Russia is much more skilful in cyber-attacking than is commonly realised and has the ability to attack critical Ukrainian infrastructure.[87] Despite this, there are military experts who think that Russia is unable to develop large cyber systems that could function in a war theatre. Thus far the US remains the sole country to have proper battlefield cyber capabilities, but many countries are eager to pursue these and to integrate them into all their military activities.[88]

Cyberwar is an integral part of Russia's hybrid warfare strategy—this is a situation the West should take seriously.

According to Limnéll, the developments in Ukraine offer a model for contemporary and future conflicts worldwide, in which a cyber element will always play an integral part[89]—cyber-attacks are currently taking place in Syria, Israel and Gaza, thus in all ongoing conflicts.

86 H. Riecke, 'Germany's Tough Hike from Summit to Summit', *La lettre de l'IRSEM* 8, 19 December 2014, 13-14.
87 S. J. Freedberg Jr., 'Russia's Information War: Latvian Ambassador, Finnish Strategist Warn On Cyber', *Breaking Defense*, 6 June 2014.
88 M. Kerttunen, 'Kybersodan keinot eivät tepsi Gazassa ja Ukrainassa' [Cyber War Methods Don't Work in Gaza and Ukraine], *Helsingin Sanomat*, 7 August 2014.
89 J. Limnéll, 'Ukraine Crisis'.

National level as the key

One size does not fit all?

In the end, many experts admit that the main risk to cybersecurity is us. Our information systems are not sufficiently protected, for instance, people do not protect their smartphones; in general there is not enough awareness of the importance of cybersecurity. Are the authorities and the national ministries that deal with sensitive information implementing adequate cybersecurity standards? The responsibility lies with the states themselves.

An EDA study shows that there is 'a mixed picture with respect to military cyber defence capability' on the national level in Europe.[90] In other words, the EU member states have very different levels of cyber capabilities and protection. The largest and most powerful member states (the UK, Germany and France) and also the medium-sized Netherlands are estimated to invest in cyber capabilities more than others. Investing in cybersecurity is not easy as, due to the abstract nature of cyber matters, the need for investment might not be straightforward to understand or explain.

Usually states' cyber defence takes place on three main levels. First, there is the technical or operational layer, such as the Computer Emergency Response Teams (CERTs),[91] which are crucial for critical information infrastructure protection. On the management or policy level, the ministries or relevant agencies come together for national coordination. Reporting then goes to the national security level, which deals with the long-term vision. NATO has a similar structure, but in the EU these layers are just beginning to be built.[92]

[90] EDA, 'EDA Study Identifies Cooperation Prospects in Cyber Defence', Press Release, 24 May 2013.

[91] All EU member states had set up national CERTs by May 2012. See an interactive map of them on the European Union Agency for Network and Information Security's (ENISA) website: https://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map.

[92] Interview with an EEAS official on 13 June 2014.

Updated intelligence legislation that enables early warning and also cross-border acquisition of information is essential.[93] The authorities should know what to do when a cyber-attack occurs, just as they know what to do when a country is attacked via land, sea or sky. In most of the EU countries this legislation is in place, despite not all member states having national cybersecurity strategies (as of April 2013 only 13 member states had adopted them). However, this is not entirely representative: in Sweden, for instance, there is no cybersecurity strategy, but cyber control is organised via other means, by the Försvarets radioanstalt (National Defence Radio Establishment). This organisation, under the control of the Ministry of Defence, follows Internet activity and gathers intelligence for the Swedish government, and is considered to be quite effective. Ergo, the size of a state's cyber components or the way they are organised does not matter, rather it is whether they work or not that is important.[94] Thus when common European criteria and standards are being implemented some room for national judgement should be allowed.

Small countries can be big in cyber, as the example of Estonia demonstrates. Prompted by the Russian cyber-attacks in 2007, Estonians created Cyber Units in their paramilitary Defence League, from which, since 2011, information and communication technology (ICT) professionals have protected the Estonian telecommunications infrastructure.[95] Since early 2014 Latvia has also had similar cyber troops (the Latvian National Guard Cyber Defence Unit), which are formed of volunteers that are committed to assisting the Latvian authorities in case of a cyber-attack. These and other out-of-the box ideas and unconventional methods of working are exactly what is needed more widely in Europe. Such innovations should be shared with other member states, for instance at Council meetings on defence. In addition to sharing best practice, the importance of cooperation in the early warning and exchange of information cannot be stressed enough when combating a threat that knows no national borders.

Updated intelligence legislation that enables early warning and also cross-border acquisition of information is essential.

[93] Interview with a national military officer on 25 June 2014.
[94] Interview with an EEAS official on 13 June 2014.
[95] For more information, see Kaitseliit, 'Estonian Defence League's Cyber Unit', last updated 2 December 2014.

Fragile trust

In cyber defence the issue of trust is imperative: countries that have trust-based relationships work better together. It is sometimes also convenient to look for partners further away than the immediate neighbourhood; for instance, Canada, the US, Australia and New Zealand have agreed to work together on cyber cooperation. According to one NATO official interviewed for this paper, it is important to remember that 'The nature of cooperation depends on context and countries. So there is no set pattern.'[96] For instance with regard to training exercises, some countries prefer bilateral ones, others multilateral ones, yet others prefer them to take place within the NATO framework, and others in the EU framework.[97] To make cooperation more attractive, it is important to find a good balance between sovereignty and security.

As a result of the EU member states' different levels of cyber capability and political ambition within the EU framework, some of the more advanced countries are not willing to develop cyber defence capabilities together in the EU framework. The reason for this is that they fear that the less well-equipped countries might endanger their own cybersecurity.[98] Some countries (namely the UK) also feel that they have invested too much money in their own cybersecurity to share it with others.[99] To some extent this is understandable, but the better-resourced countries will only be safe if all member states are on more or less the same level, as the chain is only as strong as its weakest link. It is a vicious circle, because with deeper cooperation (through EU regulation) the differences would be smaller. The imbalance in capabilities between the Allies and therefore the distrust that is visible in the EU are also present within NATO.[100] Cooperation cannot be enforced by NATO as it only offers a platform for coming together. As a NATO official regretfully noted in an interview for this paper, 'We can share best practices but we cannot establish a norm. If the members don't take part, it's they who'll lose out in the end.'[101]

96 Interview with a NATO official on 25 June 2014.
97 Ibid.
98 Interview with a national military officer on 25 June 2014 and interview with an EEAS official on 13 June 2014.
99 Interview with a European Commission official on 27 May 2014.
100 Interview with a national military officer on 25 June 2014.
101 Interview with a NATO official on 25 June 2014.

This distrust has been most visible in the transatlantic relationship, due to the 2013 revelation that the US National Security Agency had spied on European leaders. Despite this, Europe needs to get on well with the US, since working without American technology is not possible.[102] There is a good basis for co-operation as the EU and the US largely agree that fighting cybercrime and protecting critical infrastructure are top priorities, and they work well together in coordinating activities between the different CERTs.[103] The EU–US Working Group on Cyber-Security and Cyber-Crime, formed in 2010, is an important forum for cooperation, as the EU and the US are the biggest sources of both cyberspace and Internet users. For both parties to fully benefit from transatlantic cooperation there needs to be mutual respect and clear rules based on reciprocity and symmetrical rights and responsibilities. This is something that could be worked on as part of the Transatlantic Trade and Investment Partnership agreement.

The EU: versatile but uncoordinated

Narrowing the gaps

The EU aims to create a common European approach and a more level playing field among the member states, whose cyber capabilities and legislation vary significantly. There is a general consensus that more supranational cooperation is needed on cybersecurity as the cyber threat is supranational. In an interview, one military officer noted that the EU is the perfect forum for bringing together authorities from different sectors of society due to its civilian competences.[104]

The legal and policy framework in the EU concerning cybersecurity has been fragmented, but actions have been taken in two areas: improving network resilience and response capabilities. Measures have been taken to improve network and information security (NIS), critical infrastructure protection and critical

[102] Security & Defence Agenda, *Critical Infrastructure Protection in the Cyber-Age*, Report (Brussels, Summer 2014), 13.
[103] Ibid., 16.
[104] Interview with a national military officer on 22 August 2014.

information infrastructure protection, and cybercrime and cyber terrorism have also been addressed.[105] There are several bodies that deal with these issues: the European Union Agency for Network and Information Security (ENISA), the European Cyber Crime Centre, and Europol, among others.

Following on from the Internal Security Strategy in 2010 that addressed the issue of cybersecurity in the EU, the EU Cyber Security Strategy was drafted in 2013, with the goal of making the EU's online environment the safest in the world. The new strategy outlined five priorities: achieving cyber resilience, reducing cybercrime, developing an EU cyber defence policy (while avoiding duplication with NATO), developing cyber-related industrial and technological resources, and establishing an international cyberspace policy for the EU.[106]

As part of this strategy the Commission proposed a directive on NIS[107] that demands that member states put in place a minimum level of national capability by establishing national competent authorities, such as CERTs, to accompany the CERT-EU, and adopting national strategies and cooperation plans—as thus far cooperation and information sharing between the member states on NIS has taken place solely on a voluntary basis.

Businesses cannot report to the authorities anonymously, and if they feel they gain nothing in return then their motivation to report remains low.

The NIS directive aims to enable the EU to resist threats to critical infrastructure by making sure that actors in key areas such as energy, transport and banking; enablers of key Internet services; and public administrations assess the cybersecurity risks and share the information identified with the national NIS authorities, which should then regularly publish unclassified early warnings and share information on coordinated responses.[108] However, it is believed that the majority of cyber-attacks, in both the public and private sector, are not reported publicly because the information is sensitive and might undermine the reputation of the victim.[109] Businesses cannot report to the authorities

[105] P. Bąkowski, *Cyber Security in the European Union*, European Parliamentary Research Service (Brussels, 12 November 2013), 4.
[106] EEAS, 'EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity', Press Release, 7 February 2013.
[107] European Parliament and Council, *Proposal for a Directive Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, COM (2013) 48 final (7 February 2013).
[108] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final (7 February 2013), 6.
[109] European Parliament, 'Resolution on Cyber Security and Defence', L.

anonymously, and if they feel they gain nothing in return then their motivation to report remains low.[110] However, there have been promising examples of cooperation between security officials and private companies in some EU countries.

In any case, many member states still lack some of the capabilities required by the directive, and it seems many also want the rules to bind them as little as possible.[111] The EP excluded pan-European networks (such as social networks, Internet payment services and cloud service providers) from the scope of the directive altogether, so it now only focuses on state-owned companies. In spite of the challenges the legislation is facing, one interviewee noted that it is 'the first serious piece of legislation on cyber matters in the entire world, so it is remarkable.'[112] Together with the EU data protection regulation this legislation has great potential and, if successful, could be a good example for other policy areas as well.

Limited cyber defence

Although the EU Cyber Security Strategy lists cyber defence as one of its five main priorities, the EU's activities have been modest in developing the military side of cybersecurity. The EP blames the strategy, which it considers to be somewhat vague.[113] Even though the strategy includes a lot of commitments regarding defence, EU cooperation in cyber defence remains minimal on the practical level.[114] Cyber defence issues are rarely addressed at the EU level due to the EU's limited competences in Common Foreign and Security Policy and member states tend to cooperate through the NATO framework instead.[115] The EDA also admits that 'military cyber defence on the European level is at a relative early stage of maturity'.[116]

In late 2011 the EDA set up a Cyber Defence Project Team that includes 24 participating member states, and since November 2012 cyber defence has been part of the Pooling & Sharing agenda. Cyber defence

110 Interview with an assistant to an EPP MEP on 22 May 2014.
111 Ibid.
112 Interview with an EEAS official on 13 June 2014.
113 See European Parliament, *Motion for a Resolution on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013/2606(RSP) (6 September 2013); and European Parliament, *Resolution on Cyber Security and Defence*.
114 Interview with an assistant to an EPP MEP on 22 May 2014.
115 P. Bąkowski, *Cyber Security in the European Union*, 4.
116 EDA, 'EDA Study Identifies Cooperation Prospects'.

is also one of the priorities of the EDA's Capability Development Plan, which was revised in 2014. The EDA organises cybersecurity training and exercises for the member states and develops deployable cyber defence capabilities to protect EU missions, but does not do much more than this.[117] The EDA is only able to do what the member states ask of it and, unfortunately, in the framework of the CSDP, cyber defence does not extend further than EU military operations. The lack of will to take cooperation further is due to the resistance of some EU member states, with the UK at the forefront. This division between cyber cooperation in CSDP missions and national capabilities seems artificial, as basically the same capabilities are in question.[118] This problem is visible in all EU defence cooperation: the EU is mainly responsible for crisis management, and any attempt to reach a 'common defence policy' has not been given significant attention, even if it would probably require similar kinds of military capabilities as missions.[119]

However, attitudes might gradually change. The December 2013 European Council on defence mentioned cyber defence as a key capability to be developed in the EU framework,[120] and decided that an EU cyber defence policy framework needed to be drafted by the end of 2014. 'One should not expect miracles but even something concrete would be a leap forward for the EU,' observed one member of the drafting team in an interview.[121] Indeed, in November 2014 the Foreign Affairs Council adopted an EU cyber defence policy framework that 'focuses on actions to support development of member states' cyber defence capabilities that can be made available for CSDP missions', and 'sets out steps to improve the protection of CSDP communication networks managed by the EU institutions'.[122] The framework also confirms the need to reinforce research, to pool and share cyber defence training and to strengthen EU–NATO cooperation. After the adoption of the framework, the interviewee noted that even though this is a very important step forward—now for the first time a Council-level decision exists on cyber defence in the EU—it still lacks many of the elements needed. For instance,

The EU's activities have been modest in developing the military side of cybersecurity.

[117] Interview on 6 June 2014 with a journalist who specialises in defence matters.
[118] Interview with a national military officer on 25 June 2014.
[119] Missiroli, *Enabling the Future,* 53.
[120] European Council, *Conclusions*.
[121] Interview with a national military officer on 25 June 2014.
[122] Council of the European Union, '3346th Council Meeting, Foreign Affairs', Press Release 15573/14, 17/18 November 2014, 23. For further information see Council of the European Union, '"I/A" ITEM NOTE From: Political and Security Committee To: Permanent Representatives Committee (Part 2)/Council, Subject: EU Cyber Defence Policy Framework', 15193/14, 12 November 2014.

several member states were not willing to go further in information and situational-awareness sharing, and they also have somewhat different understandings of what cyber defence in the EU framework could mean. It also remains unclear what each EU institution is now tasked to do, so a more accurate roadmap needs to be drafted. Any real attempt to take cyber defence cooperation further than mere CSDP mission and structure protection is unlikely to happen soon.[123]

The EU should also consider the implications and countermeasures required if a cyber-attack should occur against an EU member state. The NIS directive proposes that in case of an attack cooperation plans are triggered and information and support is shared across the NIS authorities' network to enable the preservation or restoration of networks and services. But how would other member states react, and what countermeasures could be taken? The Lisbon Treaty's mutual defence clause[124] mentions the obligation to provide aid and assistance to a member state that is the victim of armed aggression on its territory. This threshold might not be reached by a cyber-attack, but the Lisbon Treaty solidarity clause[125] threshold might, as it mentions 'a man-made disaster', which a major cyber-attack could constitute, for instance, should the critical infrastructure of a country be shut down. The EU Cybersecurity Strategy indeed states that 'a particularly serious cyber incident or attack could constitute sufficient ground for a member state to invoke the EU Solidarity Clause',[126] even if the word 'could' leaves the situation somewhat vague. To create a credible cyber deterrent the member states need to clarify what this commitment means and lay down plans for counteraction.

Internal issues

The questions of privacy and data protection are always present when issues of cybersecurity are discussed, especially by the EP. These rights are important, and, as the EU strategy declares, for cyberspace to remain open and free, the same norms and values that the EU upholds offline, should also apply online.[127] A good balance needs to be found between these rights and security, and as MEP Tunne Kelam noted in

123 Interview with a national military officer on 15 December 2014.
124 Art. 42(7) of the Treaty on European Union.
125 Title VII, art. 222 of the Treaty on European Union.
126 European Commission, *Cyber Security Strategy of the European Union*, 19.
127 Ibid., 2.

his report, digital freedoms should be declared as fundamental rights and should not be jeopardised when responding to a cyber threat.[128] The large political groups have an understanding on this in general, however, the Greens and some MEPs from the political left are more cautious regarding cyber protection and are firmly against the EU having anything to do with defence elements.[129]

There are also institutional and capability challenges. Several EU institutions and agencies deal with cybersecurity operationally, with a light coordination mechanism and 'many of the EU entities' operational incident response functions are missing[130]—in other words they do not necessarily know what they are doing. Even an EDA study concludes that the operational setup of cyber defence between the different EU institutions involved (which include the EDA, the member states, the EEAS, the European Commission, the General Secretariat of the European Council and related EU agencies) is complex.[131] Some of the people interviewed for this paper see the EDA as the natural body to have a bigger coordinating role, 'a hub for cyber defence'.[132] But when talking about European coordination we enter into the debate about competences and the power struggles between the EU institutions, especially with and within the member states. However, several of the experts interviewed for this paper see that there is a need to coordinate efforts more and maybe even create some kind of 'EU cyber coordinator'.

[...] there is a need to coordinate efforts more and maybe even create some kind of 'EU cyber coordinator'.

The situation regarding R&D investment in cybersecurity is not inspiring. So far the Instrument for Stability is the only EU programme which can be used to deal with cyber threats.[133] This instrument is for short-term measures to react to situations of crisis or emerging crisis, usually outside Europe, when timely financial help cannot be provided from other EU sources—notwithstanding the fact that the cyber threat needs to be taken into account permanently. Horizon 2020 could bring about a change that will result in more investment in cyber-related R&D, as it will at least support security research related to emerging ICT, but this will take a while and might face national objections.

128 European Parliament, *Resolution on Cyber Security and Defence*, 5.
129 Interview with an assistant to an EPP MEP on 22 May 2014.
130 Interview with an EEAS official on 13 June 2014.
131 EDA, 'EDA Study Identifies Cooperation Prospects'.
132 Interview with an assistant to an EPP MEP on 22 May 2014.
133 European Parliament, *Resolution on Cyber Security and Defence*, 4.

The attitude towards cybersecurity in the EU should be updated. According to an EDA study, in Europe 'the culture of cyber-security good practice needs to be nurtured and the use of military specific standards and tools is still poorly understood.'[134] Furthermore there is no serious training of the staff in EU institutions on cybersecurity. In an interview one EEAS official expressed concern over this: 'There is no security culture in the EU, except maybe amongst the military staff. It will be difficult to change this.'[135]

NATO takes cyber issues to its core

NATO's wake-up call

The Russian cyber-attacks against Estonia in 2007 made NATO realise that it was not well-enough equipped against the cyber threat, even though it had worked on cyber defence for five years prior to this. As a result, NATO started to make more effort to take the cyber threat seriously:[136] organisational arrangements were implemented, such as creating the Emerging Security Challenges Division to deal with modern threats; and the organisation was developed so that cyber issues are dealt with on several levels, ranging from the political top to technical groups and international liaison.[137]

Prior to the turn of the decade NATO was slow to enhance its cyber capabilities, but since then it has moved rapidly. A revised cyber defence policy from 2011 introduced Rapid Response Teams that can be deployed within 24 hours to a member state under cyber-attack. The policy also increased continuous network protection, defined the minimum requirements for critical national networks, and launched a cyber-

134 EDA, 'EDA Study Identifies Cooperation Prospects'.

135 Interview with an EEAS official on 13 June 2014.

136 In 2008 NATO adopted its Policy on Cyber Defence, which even then mentioned assisting Allies upon request in case of a cyber-attack. In the same year the CCD COE was opened, and in 2010 the new NATO strategic concept addressed the issue of cyber threats, and was followed by a policy on cyber defence.

137 Cyber issues in NATO are dealt with on several levels and in numerous units. For more information, see NATO, 'Cyber Defence', last updated 30 September 2014.

defence exercise and training programme. Importantly, NATO included cyber issues in its defence planning in 2013—prior to that NATO had sidelined the question of deterrence and the use of force in cyberspace.[138]

The latest step was taken at its Wales Summit in September 2014 when NATO endorsed an Enhanced Cyber Defence Policy, in which Article 5 is directly linked to cyber defence for the first time: 'We affirm therefore that cyber defence is part of NATO's core task of collective defence.'[139] NATO can now send its experts to assist a country under attack[140] even though the main setting will not change: NATO will continue to be responsible for its own networks and Allies for their national networks and points of contact.[141] A new cyber-defence committee will oversee all the different cyber-defence aspects in NATO[142] and cyber defence will be more integrated in operational and contingency planning.[143] What kind of a cyber-attack would then trigger Article 5 will remain a political decision for the North Atlantic Council on a case-by-case basis—as is the procedure in a more conventional attack. This also ensures that potential attackers will not know at what point the line would be crossed. So on the whole, with the decisions made at the Wales Summit NATO's cyber defence plan is crystal clear, and has been placed at the very core of NATO's reinvigorated fundamental purpose: collective defence.

[Cyber defence] has been placed at the very core of NATO's reinvigorated fundamental purpose: collective defence.

Cyber defence will also become more integrated in NATO operations, which will affect partner countries too. Thus, as a result of the Wales Summit, cooperation with five partner countries (Finland, Sweden, Georgia, Australia and Jordan) will be deepened under the NATO Programme of Enhanced Opportunities, in which countries can freely choose the cooperation in which they wish to participate. Some non-NATO EU members have also joined or are joining the NATO CCD COE, although this is more of an academic than operative endeavour. None of these options is any substitute for full membership.

EU–NATO complementarity

138 P. Pernik, *Improving Cyber Security: NATO and the EU*, International Centre for Defence Studies (Tallinn, September 2014), 5–6.
139 NATO, 'Wales Summit Declaration', part 72.
140 Interview with a NATO military officer on 13 June 2014.
141 Interview with a NATO official on 25 June 2014.
142 Interview with a NATO military official on 25 June 2014.
143 NATO, 'Wales Summit Declaration', part 72.

When it comes to the relationship between the EU and NATO on cybersecurity, their roles are seen as somewhat complementary. In fact NATO is encouraging the EU to do more: one NATO interviewee suggested that the EU includes pan-European networks in the NIS directive, as this would reduce the amount of malware in the networks.[144]

NATO focuses on cyber defence, which is natural as NATO is directly linked to the security and intelligence organisations of its member nations. The only overlap from the EU's side might be through the work done by the EDA.[145] NATO is in a unique position as it owns its command, control, communications, computers and information systems, while the EU depends on its member states' networks for CSDP missions. Also, the EU lacks the capability to provide technical expertise and services to member states, whereas Allies can request assistance from NATO's Rapid Response Teams.[146] 'The EU simply does not have these structures—perhaps in the long term it could acquire them, but even then they might be less effective than those of NATO', was the verdict of an EEAS official in an interview.[147] The EU has other trumps: it is a legislative body that brings member states closer to the same level. According to an EP briefing, the European Commission believes that a division of labour in which NATO focuses on the military and the EU on the civilian side of cybersecurity 'is the only approach likely to be successful'.[148]

It is important that the EU does not leave all of the military side of cyber protection to NATO.

Nonetheless it is important that the EU does not leave all of the military side of cyber protection to NATO as there are many common aspects in civilian and military cyber self-protection: EU military operations are highly dependent on civilian actors and, as all defensive cyber capabilities have a dual-use potential, the EU needs to have a common civilian and military approach.[149] As one EEAS official noted, there is no point in separating civilian and military cyber capabilities, as every CSDP mission includes both and the cyber protection plan has to cover the whole entity.[150]

144 Interview with a NATO official on 25 June 2014.
145 Ibid.
146 P. Pernik, *Improving Cyber Security,* 8.
147 Interview with an EEAS official on 13 June 2014.
148 P. Bąkowski, *Cyber Security in the European Union*, 4.
149 Röhrig and Smeaton, 'Cyber Security and Cyber Defence in the European Union', 26.
150 Interview with an EEAS official on 6 June 2014

Many also believe that too much division would be rather artificial and both the EU and NATO should at least have the capability to protect their own systems, so in this sense there needs to be some duplication. As one NATO official reflected in an interview, 'The question is where you draw the line.'[151] The EU and NATO work together on issues such as cybersecurity standards in their temporary working group, but the work should be made permanent and considerably extended to include, for instance, planning, technology, training and deterrence building.

In general, concrete results from EU–NATO cooperation have so far remained modest, mainly due to the Turkey–Cyprus conflict, which has frozen official channels of cooperation.[152]

Global complications

International law and the lawless

How should cybersecurity and attacks be addressed in the framework of international law? This is very problematic as even common definitions and terminology are lacking, despite discussions in the international community. The Tallinn cyber centre, CCD COE, has written *The Tallinn Manual on the International Law Applicable to Cyber Warfare,*[153] which examines how existing international law applies to cyberspace. In 2015 a second study will be published, which aims to define the terminology and the new elements that are needed in order to apply international law in cyberspace.

The general opinion in the West seems to be that no new laws are needed for cyber issues. According to NATO, 'international law, including international humanitarian law and the UN Charter, applies in

[151] Interview with a NATO official on 25 June 2014.

[152] For more information on EU–NATO relations, see, for instance: H. Hopia, *Breaking Down the Walls: Improving EU–NATO Relations*, Centre for European Studies (Brussels, 2013).

[153] M. N. Schmitt (ed.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

cyberspace'.[154] The EU also agrees that existing legislation (the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the EU Charter of Fundamental Rights) should apply, and has not called for the creation of new legal instruments. The reasoning behind this, according to one EEAS official interviewed for this paper, is that 'some countries might use the creation of a new international cyber law to control their own people'.[155] Indeed, Russia and China surprised the international community in 2011 by putting forward a proposal for an 'International Code of Conduct for Information Security'—the hopeful sentiments of the recipients of the proposal were short-lived as it soon became clear that the code also included classifying technology such as Twitter and Facebook as 'weapons' if their use was in violation of state laws.[156]

Inadequate international cooperation only benefits hackers and their subscribers, so more has to be done globally. Some of the international cyber norms and confidence-building measures have already been strengthened, for instance via the 'London Process'[157] at high-level conferences. In 2013 it was agreed within the framework of the Organization for Security and Co-operation in Europe that there would be immediate consultations in case of a large-scale cyber-attack against a country. The EEAS is promoting this approach now in the Asia–Pacific region, and is also supporting developing countries which wish to adopt the norms of the Budapest Convention[158] in order to improve their anti-cybercrime capacity and therefore avoid the fate of becoming safe havens for cybercriminals.

It is, however, not clear how states can be made to follow international commitments. For instance, following the cyber-attacks in Estonia in 2007, a request was made by Estonia to Russia, in accordance with their mutual legal assistance treaty, to assist them with their criminal investigations. However, the response from Russia was that 'cybercrime is not a crime', and Russia was the only country out of over 70 that refused to cooperate.[159]

---

154 NATO, 'Wales Summit Declaration', part 72.

155 Interview with an EEAS official on 13 June 2014.

156 T. Farnsworth, *China and Russia Submit Cyber Proposal, Arms Control Today*, Arms Control Association (Washington, DC, November 2011).

157 There have been three annual Cyberspace Conferences since 2011, when the first conference was held in London following then UK Foreign Secretary William Hague's proposal at the 2011 Munich Security Conference. The second conference was held in Budapest (2012) and the third in Seoul (2013); the fourth will be held in The Hague in 2015.

158 The Budapest Convention is the first international treaty seeking to address Internet and computer crime, drawn up by the Council of Europe and adopted in 2001. See Council of Europe, *Convention on Cybercrime* (Budapest, 2001).

159 Interview with a former national official on 13 June 2014.

Pinpointing hackers has become easier since the Estonian experience of 2007, but if the state of origin does not cooperate, catching the attackers and people in charge will remain difficult. One idea worth considering might be to create an international cybersecurity agency, 'Cyberpol', which would have the support of major international organisations.[160] As technology advances and hackers are able to be located more accurately, it might soon be possible to hold the state of origin, if uncooperative, responsible for the attacks.

Deterrence and offensiveness

Should existing international law apply in cyberspace, the right to self-defence, and therefore counter-attack, also applies. The issue of offensive cyber measures is, however, very sensitive in Europe, and is totally absent from the EU's political discussions.[161] As experts Wolfgang Röhrig and Rob Smeaton note, 'The EU is solely engaged in cyber self-protection and assured access to cyber space to enable conventional military activity'; 'offensive cyber capabilities have not been developed, or deployed, under the EU banner.'[162] Nor is NATO, as an Alliance, preparing offensive capabilities in this regard. However, discussions on this are now taking place within NATO, which some years ago would have seemed very unlikely.[163] Regardless of the organisations' lack of enthusiasm, some NATO nations are developing these capabilities, and they could be used by the whole Alliance with an Article 5 decision.[164]

An article citing an ENISA study writes that multiple nation states are now developing capabilities that can be used to 'infiltrate all kinds of targets both governmental and private ones'.[165] The UK and the Netherlands have publicly called for stronger aggressive capabilities in cyber warfare and, according to the article, former British Defence Secretary Philip Hammond has said that 'simply building cyber defences is not enough: as in other domains of warfare, we also have to deter. Britain will build a dedicated capability to counterattack in cyberspace and if necessary to strike in cyberspace'.[166]

---

160 Friends of Europe, 'Security Jam 2014: Top 10 Recommendations', 24 November 2014, point 9.
161 Interview with an EEAS official on 13 June 2014.
162 Röhrig and Smeaton, 'Cyber Security and Cyber Defence in the European Union', 24.
163 Interview with a NATO military officer on 13 June 2014.
164 Interview with a national military officer on 25 June 2014.
165 J. Fleming, 'EU Nations Developing Cyber "Capabilities" to Infiltrate Government, Private Targets', *EurActiv.com*, 12 December 2013.
166 Ibid.

But is it enough that some member states are doing this on their own? Should there not be at least a discussion on the European level? The question of how to create a cyber deterrent is not a simple one. One estimate from a private sector representative is that traditional deterrence does not necessarily work in cyberspace as the tools are not physical weapons.[167] Another concern is that if counterattacking, we might reveal too much of ourselves to the adversary.[168] However, others argue that the deterrent actually already exists: there have been no strategic cyber campaigns causing 'large-scale destruction, loss of life or economic impact similar to that from a military attack', because the most capable cyber nations have assessed that it is not worth the potential punishment.[169]

Europe's economic future

Cooperation with the private sector is essential to beat the cyber threat—this is because businesses own the cyber-protection capabilities and also most of the infrastructure that might be the target of a cyber-attacker. NATO is something of a beginner in this as its structures are not set up for interaction with businesses, but this might soon change as NATO adopted a new Industry Cyber Partnership in Wales.[170] However, the EU is applauded on this front—according to a private sector representative—as the ENISA permanent stakeholder group is a very effective form of cooperation, where experts from the private sector advise the decision-making body of the agency, with meetings taking place on a regular and transparent basis.[171]

Better cyber protection and better tools would increase the trust of businesses and consumers in digital commerce, and would create more jobs.

Investing in cybersecurity and cooperating with businesses would also bring wider economic benefits if there was a functioning and reliable European Digital Single Market, which is one of new Commission President Jean-Claude Juncker's priorities. This should already be enough to encourage member states to address the need for better cyber protection, as the Digital Single Market will not work without secure

167 Interview with a private sector representative on 28 August 2014.
168 Interview with an EEAS official on 6 June 2014.
169 J. Healey, 'Commentary: Cyber Deterrence is Working, Dynamics are Similar to the Cold War Nuclear Standoff', *DefenseNews.com*, 30 July 2014.
170 NATO, 'Wales Summit Declaration', part 72.
171 Interview with a private sector representative on 28 August 2014.

networks and clear data protection rules. To make the European digital environment the safest in the world and to establish global leadership in cybersecurity standardisation, European standardisation bodies have called for the EU to create a harmonised European cybersecurity standard.[172] Better cyber protection and better tools would increase the trust of businesses and consumers in digital commerce, and would create more jobs.

What is problematic from the EU's point of view is that Europe is no longer producing ICT. Therefore, there is no certainty that, for instance, mobile phone chips have not already been corrupted when they enter Europe. More R&D investment should be allocated to address ICT shortfalls, and the EU Cybersecurity Strategy stresses the need for appropriate cybersecurity performance requirements to be implemented across the whole value chain for ICT products used in Europe.[173] However, one EEAS official interviewed for this paper worries that 'Not all European countries can afford to supervise the supply chain or clean the devices'.[174] Other interviewees also expressed concern: 'I think the new concepts and technologies will be invented in North America, mass produced in Asia and used in Europe', said one NATO official.[175] An EP official summarised the situation: 'The US thinks globally and about influence. We don't.'[176] A private sector representative offered the solution: 'If the technology is already out, you've lost it. To compete in a sector, you have to find what we call a Blue Ocean, an area where one can gain a competitive advantage.'[177]

[172] Cyber Security Coordination Group CEN/CENELEC/ETSI, *Recommendations for a Strategy on European Cyber Security Standardisation*, White Paper no. 1, version 01.08, (Berlin, 21 March 2014), 4.
[173] EU, *Cybersecurity Strategy of the European Union*, 12.
[174] Ibid.
[175] Interview with a NATO official on 25 June 2014.
[176] Interview with an assistant to an EPP MEP on 22 May 2014.
[177] Interview with a private sector representative on 28 August 2014.

Conclusions

When technological developments change the system profoundly, we can talk about disruptive technologies; RPAS, or drones, and cyber issues represent a contemporary case. These technologies are now available, not only to states, but to various actors. Moreover, they are not expensive, which ensures that their proliferation will be rapid. We should not talk about new threats, but about more diverse, multifaceted and efficient methods of carrying them out. RPAS and cyber-attacks are both at the core of modern and future warfare. Europe must be prepared for these tools to be used against it, but it must also develop these technologies for itself. These technologies have both civilian and military aspects and can be used to benefit both European security and the economy.

Unfortunately, Europe has fallen behind in the technological race, and EU research money has been kept away from defence-related initiatives. There are grave capability shortfalls in European military technologies and equipment, such as those in surveillance and reconnaissance capabilities. Europe has been too comfortable relying on help in operations and procurement from outside Europe, especially from the US. But Europe simply cannot afford to continue on this path, particularly when it is facing the current alarming security situation with Russia waging war in Ukraine.

There are grave capability shortfalls in European military technologies and equipment, such as those in surveillance and reconnaissance capabilities.

It is encouraging to see that the EU and NATO have taken some steps forward. In December 2013, the European Council decided to prepare for the arrival of European MALE drones by 2015–20. A European approach to drones would bring cost-effectiveness and operational advantages from working together, increase European self-sufficiency, and revitalise the European defence industry, which has suffered from a lack of programmes. The EU is now harmonising the regulatory landscape to enable these European projects, and NATO is involved in providing standardisation and training. But the will to invest in defence-related R&D, in order to maintain the European defence industry and to take part in EU-level projects, has to come from the member states themselves.

Europeans need to address the cyber threat since their countries, with large industries and a good deal of intellectual property, are very vulnerable to attacks. NATO estimates that the impact of a cyber threat could potentially be as high as that of a conventional attack. The safety of cyberspace is also important for the economic future of Europe, as there cannot be a trustworthy Digital Single Market without secure net-

works—the inclusion of private companies in this work is essential. Cybersecurity is also important when it comes to other technologies, such as RPAS. Cyber-attacks can vary from crime to espionage and to use as a weapon in war.

Both the EU and NATO have acknowledged cybersecurity as a strategic priority, but the member states remain responsible for their own national cybersecurity. The EU has focused mainly on cybercrime and narrowing the gap in security between the member states; the NIS directive introduces minimum levels for national capabilities, authorities, strategies and plans. The EU's work on cyber issues takes place in several institutions and units, so a coordinating authority could be useful. NATO focuses solely on the military side of cybersecurity and at its summit in Wales in September 2014 the Alliance agreed to include cyber defence in the collective defence concept. The roles of the two organisations in cybersecurity are mostly complementary; however, the EU also needs to have a strong role in cyber defence. The EU is working on this; foreign ministers adopted an EU cyber-defence policy framework in November 2014, but it seems that cyber defence will mostly continue to be linked only to CSDP mission protection, not, for instance, covering situational-awareness sharing. The member states also have varying understandings of what cyber defence in the EU framework would mean. The EU and NATO should further their cyber cooperation and also discuss the question of cyber deterrence and offensive capabilities; however this seems to be difficult due to problems at the official level.

More political will is needed to step up the efforts that are necessary for Europe's security, and political parties have a decisive role in the generation of this will.

The disruptive technologies examined in this research paper bring up new concerns, such as privacy and the applicability of international law in relation to both RPAS and cyber-attacks. With RPAS there are also concerns over the rules of engagement, human responsibility and transparency. But with lessons learned and proper EU and international laws and rules, these concerns should not hinder Europe's use of armed drones—RPAS should be considered similarly to any other device that can be used for many purposes and either in the wrong or the right way. In cybersecurity both the EU and NATO believe that existing international law should also apply online, as changes might be exploited by some states who want to tighten control over their citizens. Common international terminology and norms should be put in place, and mechanisms to locate and penalise cyber-attackers need to be developed.

The work is underway, but it remains to be seen whether concrete actions will follow. The EU's progress will be assessed at the European Council in June 2015 and the new Commission leadership and the EP have a responsibility to demand that the member states stay true to their commitments. Too often the member states do not see the full potential of cooperation, but stick to the idea that they can manage by themselves, only want to protect their national interests or simply do not trust each other enough to cooperate. 'The Westphalian state system has not disappeared', as one NATO official put it. It is important that a country's own interests are looked after, but not when that hampers the common interest, and thus, in the end, its own as well.

One problem, according to many interviewees, is that Europeans tend to see defence issues as something to avoid getting involved in, regardless of the worrying times. To succeed, or to survive even, we have to increase our understanding of the rapidly changing world, adapt and develop a more strategic way of thinking together. New technologies are also too often feared, when instead we should embrace them, as they not only pose threats but also offer great opportunities. More political will is needed to step up the efforts that are necessary for Europe's security, and political parties have a decisive role in the generation of this will. As a responsible political actor and the largest political group in Europe, the EPP should take the lead. We have to raise the anchor because at the moment we are stuck in the harbour, when we should desire to sail off into the blue sea, our future.

Policy recommendations

General guidelines

Assess the changing security environment, prepare for contemporary threats.

Europe needs to be alert to security changes in its neighbourhood and invest in defence again. In the currently impaired European security environment caused by Russian aggression this should be self-evident to all decision-makers. The nature of contemporary threats, such as hybrid war, has to be understood and capabilities have to be up-to-date to address them—the more self-sufficient and capable Europe is in its defence, the less likely it is to be threatened by potential aggressors. Europe should also prepare for the diffusion of power and proliferation of technology: in the future an increasing number of different actors will be able to access disruptive devices and might also use them as weapons against Europe.

Increase awareness of disruptive technologies. Discuss the concerns they bring about and offer solutions through a concrete legislative framework.

People fear what they do not know. The EU should fight prejudices related to RPAS, cyber tools and other similar technologies, which, in addition to being able to cause destruction, can also be used for protection and many sorts of aid and assistance, and have commercial benefits via civilian applications. Concerns relating to disruptive technologies such as privacy, the rules of engagement, transparency and humanitarian issues have to be tackled through common rules and legislation. Europe should commit itself to the rules and to international and humanitarian law when using disruptive technologies, learning from past lessons. It should work in the international arena to enforce international norms and rules, because some actors might misuse the current vague setting. Promoting an international agreement on these rules is in Europe's best interest.

The EU has to be more strategic in its thinking. An EU white paper on defence is much needed and should also deal with disruptive technologies.

The EU needs to draft a white paper on defence that, instead of merely describing the security environment, includes the EU's strategic vision, responses in case of the materialisation of threats and capability assessments. The EU should work as closely as possible with NATO on this strategic approach. The EU should clarify how to secure its essential systems when countering a threat and how the EU's solidarity and mutual defence clauses would apply—and have member states commit to this. For instance, in the case of a cyber-attack against an EU member state, what are the thresholds and common actions? This is a relevant question, as not all EU member states belong to NATO. Disruptive technologies have to be at the core of this strategic paper and they need to be assessed together as, for instance, drones need cyber protection to be able to function. A comprehensive security approach is necessary, in which disruptive technologies that have both civilian and military aspects are included.

Clarify institutional responsibilities, increase EU-level cooperation and pressure the member states to deliver on their commitments.

The political and institutional setting can no longer remain fragmented, as important resources are being wasted. Instead of focusing on competences and power struggles, the objective should be to solve problems. The EU should increase cooperation when tackling common threats—they cannot be addressed alone in an uncoordinated fashion. The European Commission and the EP have to ensure that the member states stay committed to the decisions taken by the European Council in December 2013—especially concerning cyber defence and the European MALE drone—and that concrete steps are taken; the developments should be evaluated at the June 2015 European Council and regularly thereafter. Member states are responsible for keeping their national defence systems up-to-date, adequately funded and able to address a large variety of threats—these matters need to be regularly discussed and, when needed, coordinated, at the EU level.

Clarify and intensify EU–NATO cooperation.

The EU and NATO should intensify cooperation and consultations and introduce joint planning when it comes to tackling hybrid warfare and threats brought on by new technologies. The EU and NATO should explore the possibility of working together on a cyber-protection strategy, bringing in their respective strengths. They should also address the questions of what constitutes a credible cyber deterrent and what offensive measures are required. Concerning RPAS, possible synergies and cooperation between the EU and NATO should be examined, for instance in the format of the Berlin Plus agreement.

Invest in technologies, innovations and also defence-related R&D.

The EU should increase awareness of technological developments and the need to invest in them, and retain adaptability and resilience. The EU should make up for lost time as soon as possible, and start rapidly investing in R&D, innovation, and technology. The EU should encourage member states to take the issue of defence funding seriously and demand that they fulfil defence R&D funding commitments. It should also enable EU-funded defence research as part of the Multiannual Financial Framework for 2021–7 and explore ways to allocate funding for this purpose in the EU's annual budgets. The EU's financial instruments should have enough flexibility for urgent funding if needed in specific cases. A comprehensive EU-level research strategy could bring together the national work on dual-use and defence-related research programmes.

Identify and tackle European capability shortfalls in defence and new technologies in a coordinated manner, develop a better-functioning European defence market.

The member states and the EDA should work better together to pinpoint capability shortfalls and overcapacities to see how European and national resources could best be used. The sectors and capabilities where the EU or European NATO nations are dependent on external resources should be mapped out, and strategies and action plans needed to become more self-reliant should be considered. The EDA should be allowed to evolve into a true defence agency that carries out real procurement, and countries not willing to accept this should stay out of it. The EDA's budget needs to be unfrozen so that the Agency can start to carry out its tasks. In its defence-related projects the EU should always take into account the European single market, the European defence market and the business opportunities these technologies represent

for European companies. It should create the legislative and political conditions for the European defence industry to gain strength—this is important for European self-sufficiency and its economy.

Concrete actions on RPAS

Acknowledge the advantages of RPAS.

RPAS have great operational capacities and are valuable in surveillance, information gathering and military operations. They eliminate the endangering of the lives of one's own pilots, and are more accurate and provide good vision, consequently reducing the risk of collateral damage. RPAS are cost-effective to produce and can be used for several purposes, both civilian and military, and increasingly for commercial ones too—the opportunities for job creation are endless. A European drone also capable of combat missions would save resources, offer operational and cooperative advantages, and increase Europe's self-sufficiency.

Create a clear rule framework and learn from the past to tackle fear and prejudices.

Concerns about matters such as privacy, transparency, the rules of engagement and respect for international law have to be clearly taken into account. The experiences from previous drone missions, such as American ones, should be taken on board. European missions should be carried out following an agreed set of rules, under political supervision and always with a human being making the decision to engage in combat. International legal frameworks should be clear and Europe needs to follow these in order to expect the same from others. When the rules are followed, RPAS can be considered in the same way as any other device that can be used for multiple purposes.

Implement European legislation and regulations with the goal of fully realising the dual-use potential of European MALE RPAS.

The EU should make sure EU member states implement the common requirements, rules, standards and certificates, and follow what they have committed to. It should underline the commitment by the member states to create a European MALE drone, include the EU/EDA framework as closely as possible in the project and encourage as many member states as possible to get involved. The EU should explore the areas where RPAS could potentially be of even more value, in different military or civilian functions and in business; it should also use a dual-use approach to advance the defence side of RPAS. Moreover, the EU needs to identify and prepare for the threat scenarios that the proliferation of RPAS could create, for instance, through their use by terrorists or other hostile actors in Europe.

Concrete actions on cyber defence

Address the lack of cyber-awareness on all levels, and work intensively with the private sector to capitalise on developments in cyber security.

The EU should include cybersecurity as an overarching approach and basic necessity in all EU institutions and public administrations in the member states. It should introduce training in cyber matters for staff and public education programmes, and also ensure that it is taught at universities. Cooperation with the private sector in cybersecurity should be increased and the EU should listen to the ICT industry, as it has the expertise. Information should be shared faster and businesses' anonymity should be guaranteed when reporting attacks. When possible, European companies should be contracted, instead of purchasing equipment and know-how from elsewhere. The European Digital Single Market should be completed and the need to have more secure networks in order to be able to do so should be acknowledged.

Ensure member states reach agreed criteria in cyber protection, bridge the gaps between member states, improve the cybersecurity of EU structures and EU operations.

Member states need to complete the commitments contained in the EU Cybersecurity Strategy, the NIS directive and the EU cyber defence framework. National competent authorities, national strategies and cooperation plans need to be updated; and a cyber element needs to be included in their crisis management plans—thus increasing overall security and the possibility of building more trust between the member states. It should be possible for member states to make some national adjustments, but only if these do not hamper the overall common objectives. The member states should see more opportunities in the pooling and sharing of cyber defence capabilities. The EU and NATO should ensure that all components of their operations enjoy a high level of cyber protection, and also that their headquarters and networks are fully protected.

Coordinate cyber security efforts better by evaluating cyber preparedness, bringing together cyber capabilities, and sharing information and situational awareness.

The EU should continuously evaluate the preparedness of the institutions and member states to tackle cyber-attacks, and estimate where more protection and cooperation are needed. Convergence in the strategic planning of the cyber defence requirements of the member states needs to be enhanced (in areas such as monitoring, situational awareness, prevention, detection and protection, information sharing, forensics and malware analysis capabilities, and lessons learned). The EU should consider creating an 'EU cyber coordinator', who brings together all aspects of cyber matters—crime prevention, defence and diplomacy—who would potentially reside within the EEAS and would help to create a common understanding of the different cyber definitions, such as the concept of cyber defence in the EU. The EU should consider extending EU cyber defence cooperation further than just the operational context, to also include information and situational-awareness sharing, which would put it on a path towards creating a common cyber defence policy. Within the EU the meanings and responses concerning the mutual defence and solidarity clauses should be clarified in case of a cyber-attack.

Strengthen the links between NATO and the EU (especially the EDA) on cyber defence.

EU–NATO working level meetings should take on a more permanent structure, where information and best practices can be exchanged and better cyber deterrence can be built. EU–NATO cooperation on cyber defence could set a valuable example for improved cooperation, based on respective strengths, between the two organisations. More cooperation could be achieved for instance in cyber-defence training, capability building and in operations; also the respective response teams or units should work more closely together to increase common situational awareness and information sharing. EU–US cooperation should also continue, based on mutual respect and reciprocity.

Continue work on the international level to define the terminology, norms, rules and laws concerning cybersecurity.

The EU should promote anti-cybercrime policies and the Budapest Convention, and continue to help developing countries protect themselves against the cyber threat. Cyber rules should be promoted more determinedly in the international arena by working together with relevant partners and upholding international law. The responsibilities of states in the apprehension of cyber-attackers should be made clear. Common efforts could be strengthened by creating an international cybersecurity agency or a similar strategy.

Acknowledgments

This research paper is based on desk study and over a dozen separate off-the-record interviews with institutional or national officials and other experts. The author would like to thank all the individuals and organisations that have contributed to this work.

Bibliography

Akamai Technologies, *Akamai's State of the Internet, Q1 2014 Report,* vol. 7, no. 1 (2014), accessed at http://www.akamai.com/dl/akamai/akamai-soti-a4-q114.pdf?WT.mc_id=soti_Q114 on 6 September 2014.

Bąkowski, P., *Cyber Security in the European Union,* European Parliamentary Research Service (Brussels, 12 November 2013), accessed at http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf on 12 May 2014.

Bower, J. L. and Christensen, C. M., 'Disruptive Technologies: Catching the Wave', *Harvard Business Review* (January/February 1995), 43–53, accessed at http://catalogue.polytechnique.fr/site.php?id=576&fileid=6845 on 16 June 2014.

Brimley, S., FitzGerald, B. and Sayler, K., *Game Changers. Disruptive Technology and U.S. Defense Strategy,* Center for a New American Security, Disruptive Defence Papers (Washington, DC, September 2013), accessed at http://www.cnas.org/files/documents/publications/CNAS_Gamechangers_BrimleyFitzGeraldSayler_0.pdf on 18 April 2014.

Byman, D., 'Why Drones Work. The Case for Washington's Weapon of Choice', *Foreign Affairs,* July/August 2013, accessed at http://www.foreignaffairs.com/articles/139453/daniel-byman/why-drones-work on 13 November 2014.

Charillon, F., 'Guerres hybrides et processus décisionnels incertains', Editorial, *La lettre de l'IRSEM* 8, 19 December 2014, 1–2, accessed at http://www.defense.gouv.fr/content/download/333076/4619493/file/Lettre_IRSEM_n8_2014.pdf on 23 December 2014.

Christensen, C. M., *The Innovator's Dilemma* (Cambridge, MA: Harvard Business School Press, 1997).

Coelmont, J. and Biscop, S., *Building European Defence: An Architect and a Bank,* Egmont Royal Institute for International Relations, Security Policy Brief no. 56 (Brussels, May 2014), accessed at http://www.egmontinstitute.be/wp-content/uploads/2014/05/SPB56.pdf on 12 May 2014.

Council of Europe, *Convention on Cybercrime* (Budapest, 2001), accessed at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm on 11 December 2014.

Council of the European Union, '"I/A" ITEM NOTE From: Political and Security Committee To: Permanent Representatives Committee (Part 2)/Council, Subject: EU Cyber Defence Policy Framework', 15193/14 (12 November 2014), accessed at http://data.consilium.europa.eu/doc/document/ST-15193-2014-INIT/en/pdf on 12 December 2014.

Croft, A. and P. Apps, 'NATO Websites Hit in Cyber Attack Linked to Crimea Tension', *Reuters*, 16 March 2014, accessed at http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316 on 22 May 2014.

Cronin, A. K., 'Why Drones Fail. When Tactics Drive Strategy', *Foreign Affairs,* July/August 2013, accessed at http://www.foreignaffairs.com/articles/139454/audrey-kurth-cronin/why-drones-fail on 10 November 2014.

Cyber Security Coordination Group CEN/CENELEC/ETSI, *Recommendations for a Strategy on European Cyber Security Standardisation,* White Paper no. 1, version 01.08 (Berlin, 21 March 2014), accessed at http://www.cscg.focusict.de/sixcms_upload/media/3829/CSCG%20White%20paper.171536.pdf on 11 November 2014.

Davis, Jr., J. R., 'U.S. Army: Defeating Future Hybrid Threats. The Greatest Challenge to the Army Profession of 2020 and Beyond', *Military Review* (September/October 2013), 21–9, accessed at http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20131031_art006.pdf on 10 September 2014.

Davis, L. E. et al., *Armed and Dangerous? UAVs and U.S. Security,* RAND Corporation (Santa Monica, California, 2014), accessed at http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR449/RAND_RR449.pdf on 23 September 2014.

EDA, 'Defence Ministers Commit to Capability Programmes', Press Release, 19 November 2013, accessed at http://www.eda.europa.eu/info-hub/news/2013/11/19/defence-ministers-commit-to-capability-programmes on 18 April 2014.

EDA, 'EDA Study Identifies Cooperation Prospects in Cyber Defence', Press Release, 24 May 2013, accessed at https://www.eda.europa.eu/info-hub/news/press-releases/2013/05/24/eda-study-identifies-cooperation-prospects-in-cyber-defence on 25 June 2014.

EEAS, 'EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity', Press Release, 7 February 2013, accessed at http://europa.eu/rapid/press-release_IP-13-94_en.htm on 13 June 2014.

EEAS, *Preparing the December 2013 European Council on Security and Defence, Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy* (Brussels, 15 October 2013), accessed at http://eeas.europa.eu/statements/docs/2013/131015_02_en.pdf on 28 April 2014.

European Commission, *A New Deal for European Defence, Towards a More Competitive and Efficient Defence and Security Sector,* Communication, COM (2013) 542 final (24 June 2014), accessed at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0542:FIN:EN:PDF on 11 December 2014.

European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN(2013) 1 final (7 February 2013), accessed at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf on 12 May 2014.

European Commission, 'European Commission Calls for Tough Standards to Regulate Civil Drones', Press Release, 8 April 2014, accessed at http://europa.eu/rapid/press-release_IP-14-384_en.htm?locale=en on 8 April 2014.

European Commission, *Towards a More Competitive and Efficient Defence and Security Sector,* Communication, COM (2013) 542 final (24 July 2013), accessed at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013DC0542&from=EN on 11 December 2014.

European Council, *Conclusions,* EUCO 217/13 (20 December 2013), accessed at http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf on 28 January 2014.

European Parliament and Council Directive 2009/43/EC simplifying terms and conditions of transfers of defence-related products within the Community (Text with EEA relevance), OJ L146 (6 May 2009), 1.

European Parliament and Council Directive 2009/81/EC on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC (Text with EEA relevance), OJ 216 (13 July 2009), 76.

European Parliament and the Council of the European Union, *Proposal for a Directive Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union,* COM (2013) 48 final (7 February 2013), accessed at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666 on 13 June 2014.

European Parliament, *Joint Motion for a Resolution on the Use of Armed Drones,* 2014/2567(RSP) (25 February 2014), accessed at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+P7-RC-2014-0201+0+DOC+PDF+V0//EN on 18 April 2014.

European Parliament, *Motion for a Resolution on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* 2013/2606(RSP) (6 September 2013), accessed at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B7-2013-0386+0+DOC+PDF+V0//EN on 12 May 2014.

European Parliament, *Resolution on Cyber Security and Defence*, 2012/2096(INI) (22 November 2012), accessed at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0457+0+DOC+PDF+V0//EN on 22 May 2014.

Farnsworth, T., *China and Russia Submit Cyber Proposal, Arms Control Today,* Arms Control Association (Washington, DC, November 2011), accessed at https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal on 10 September 2014.

Fleming, J., 'EU Nations Developing Cyber "Capabilities" to Infiltrate Government, Private Targets', *EurActiv.com,* 12 December 2013, accessed at http://www.euractiv.com/infosociety/eu-nations-lack-common-approach-news-532294 on 13 May 2014.

Freedberg, Jr., S. J., 'Russia's Information War: Latvian Ambassador, Finnish Strategist Warn On Cyber', *Breaking Defence,* 6 June 2014, accessed at http://breakingdefense.com/2014/06/russias-information-war-latvian-ambassador-finnish-strategist-warn-on-cyber/ on 20 October 2014.

Friends of Europe, 'Security Jam 2014: Top 10 Recommendations', 24 November 2014, accessed at http://www.friendsofeurope.org/security-defence-agenda/security-jam-2014-top-10-recommendations/ on 12 December 2014.

Frontini, A., 'Beyond the "Guns or Butter" Dilemma – The December European Council and the Future of the European Defence Industry', European Policy Centre, Commentary (Brussels, 4 December 2013), accessed at http://www.epc.eu/pub_details.php?cat_id=4&pub_id=3981&year=2013 on 12 May 2014.

Grevi, G. et al., *Empowering Europe's Future: Governance, Power and Options for the EU in a Changing World* (European Union, 2013), accessed at http://europa.eu/espas/pdf/espas-report-governance-power.pdf on 18 June 2014.

Healey, J., 'Commentary: Cyber Deterrence is Working, Dynamics are Similar to the Cold War Nuclear Standoff', *DefenseNews.com,* 30 July 2014, accessed at http://www.defensenews.com/article/20140730/DEFFEAT05/307300017/Commentary-Cyber-Deterrence-Working on 12 November 2014.

Hopia, H., *Breaking Down the Walls: Improving EU–NATO Relations,* Centre for European Studies (Brussels, 2013), accessed at http://martenscentre.eu/sites/default/files/publication-files/livret_eu-nato_links.pdf on 11 December 2014.

Intel Security, *Net Losses - Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II* (Santa Clara, California, June 2014), accessed at http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf on 7 September 2014.

International Security Information Service Europe, 'Parliamentary Update no. 56, SEDE Subcommittee', 12 February 2014, accessed at http://isis-europe.eu/wp-content/uploads/2014/08/pu141.pdf on 12 May 2014.

Joint Air Power Competence Centre, *Remotely Piloted Aircraft Systems in Contested Environments: A Vulnerability Analysis* (Kalkar, September 2014), accessed at http://www.japcc.org/publications/report/Report/JAPCC_RPAS_In_Contested%20_Environements.pdf on 20 October 2014.

Jones, S., 'Nato Summit on "High Alert" for Cyber Attack', *Financial Times*, 3 September 2014, accessed at http://www.ft.com/intl/cms/s/0/bd29b7b6-335a-11e4-9607-00144feabdc0.html#axzz3D42v1KaO on 9 September 2014.

Jones, S., 'Russian Government Behind Cyber Attacks, Says Security Group', *Financial Times*, 28 October 2014, accessed at http://www.ft.com/intl/cms/s/0/93108ba0-5ebe-11e4-a807-00144feabdc0.html?siteedition=intl#axzz3lyy7c4wC on 13 November 2014.

Jones, S., 'Ukraine PM's Office Hit by Cyber Attack Linked to Russia', *Financial Times*, 7 August 2014, accessed at http://www.ft.com/intl/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0.html?siteedition=uk#axzz3D42v1KaO on 6 September 2014.

Kaitseliit, 'Estonian Defence League's Cyber Unit', last updated 2 December 2014, accessed at http://www.kaitseliit.ee/en/cyber-unit on 11 December 2014.

Kerttunen, M., 'Kybersodan keinot eivät tepsi Gazassa ja Ukrainassa' [Cyber War Methods Don't Work in Gaza and Ukraine], *Helsingin Sanomat,* 7 August 2014, accessed at http://www.hs.fi/paakirjoitukset/a1407302111965 on 7 August 2014.

Lentz, J. P., 'A Roadmap for RPAS Integration in European Airspace by 2016', presentation at the European Commission Directorate-General Enterprise and Industry, ASD Convention Technology Forum, Lisbon, 11 October 2012, accessed at http://www.asd-europe.org/fileadmin/user_upload/Client_documents/ASD_Contents/2_COMMUNICATION/2.5_Publications/2.5.5_Speeches_and_Presentations/2.5.5.1_

ASD_Convention_Technology_Forum_2013/Technology_Forum/Business/A_Roadmap_for_RPAS_Integration_in_European_Airspace_by_2016.pdf on 12 September 2014.

Limnéll, J., 'Ukraine Crisis Proves Cyber Conflict is a Reality of Modern Warfare', *The Telegraph,* 19 April 2014, accessed at http://www.telegraph.co.uk/technology/internet-security/10770275/Ukraine-crisis-proves-cyber-conflict-is-a-reality-of-modern-warfare.html on 20 October 2014.

Michel, L., 'An American Perspective on the Wales Summit: Now Comes the Hard Part', *La lettre de l'IRSEM* 8, 19 December 2014, 9–10, accessed at http://www.defense.gouv.fr/content/download/333076/4619493/file/Lettre_IRSEM_n8_2014.pdf on 23 December 2014.

Missirolli, A. (ed.), *Enabling the Future – European Military Capabilities 2013–2025: Challenges and Avenues,* EU Institute for Security Studies (Paris, 2013), accessed at http://www.iss.europa.eu/uploads/media/Report_16.pdf on 15 September 2014.

NATO, 'NATO Alliance Ground Surveillance Programme takes off in Chicago', Press Release, 21 May 2012, accessed at http://www.nato.int/cps/en/natohq/news_87544.htm?selectedLocale=en on 14 November 2014.

NATO, 'Wales Summit Declaration', Press Release, 5 September 2014, accessed at http://www.nato.int/cps/en/natohq/official_texts_112964.htm on 5 September 2014.

Pernik, P., *Improving Cyber Security: NATO and the EU,* International Centre for Defence Studies (Tallinn, September 2014), accessed at http://www.icds.ee/fileadmin/media/icds.ee/reports/Piret_Pernik_-_Improving_Cyber_Security.pdf on 22 October 2014.

Reuters, 'Armed UK Drones Deployed in Iraq, Support Fight against ISIS', 16 October 2014, accessed at http://rt.com/uk/196508-reaper-drones-iraq-isis/ on 21 October 2014.

Riecke, H., 'Germany's Tough Hike from Summit to Summit', *La lettre de l'IRSEM* 8, 19 December 2014, 13–14, accessed at http://www.defense.gouv.fr/content/download/333076/4619493/file/Lettre_IRSEM_n8_2014.pdf on 23 December 2014.

Robinson, N. et al., *Security Challenges to the Use and Deployment of Disruptive Technologies,* RAND Europe (Santa Monica, California, 2007) accessed at http://www.rand.org/content/dam/rand/pubs/technical_reports/2007/RAND_TR406.pdf on 16 June 2014.

Röhrig, W. and Smeaton, R., 'Cyber Security and Cyber Defence in the European Union, Opportunities, Synergies and Challenges', *Cyber Security Review* (Summer 2014), 23–7, accessed at https://www.eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf on 14 November 2014.

Schmitt, M. N. (ed.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), accessed at http://issuu.com/nato_ccd_coe/docs/tallinnmanual on 11 December 2014.

Security & Defence Agenda, *Critical Infrastructure Protection in the Cyber-age,* Report (Brussels, Summer 2014), accessed at http://www.friendsofeurope.org/media/uploads/2014/10/FoE-Report-Critical-Infraestructure-protection-in-the-cyber-age-WEB.pdf on 20 August 2014.

Stothard, M. and Parker, A., 'Airbus Chief Calls for United EU Drone Project', *Financial Times,* 16 July 2014, accessed at http://www.ft.com/intl/cms/s/0/fe809cb6-0cfe-11e4-bf1e-00144feabdc0.html#axzz38tViuXZX on 29 July 2014.

Summers, D. J., 'Fighting in the Cyber Trenches', *Fortune,* 13 October 2014, accessed at http://fortune.com/2014/10/13/cold-war-on-business-cyber-warfare/ on 10 November 2014.

Wheeler, N., 'Remote Control: Remotely Piloted Air Systems', UK Parliament website, November 2013, accessed at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmdfence/writev/772/rpa21.htm on 11 December 2014.

Wortzel, L. M., *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, Testimony of Larry M. Wortzel before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations,* Summary of Testimony (Washington, DC, 9 July 2013), accessed at

http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf on 14 November 2014.