SWP Comments

Stiftung
Wissenschaft und
Politik

German Institute
for International and
Security Affairs

The New 'Europe of Security'

Elements for a European White Paper on Security and Defence

Annegret Bendiek

With the Estonian Presidency of the EU Council from July until December 2017, the main topics will be digitalization and "a safe and secure Europe". The Council Presidency will, therefore, be tackling Europe's major challenges. At the same time, it can make use of a wide-open window of opportunity, since the governments of the EU Member States are more willing than ever to consider deepening European foreign and security policy. The issue of security has also been a constant concern for the Commission since the beginning of its term – from President Juncker's Political Guidelines in July 2014 to his most recent State of the Union Address in September 2016. Politics and society support a 'Europe of Security' based on three major projects of current European policy: a security union, a defence union and close cooperation between NATO and the EU. When protecting critical infrastructures, i.e. cybersecurity, these projects merge. All three should be given a shared strategic vision in an overarching White Paper.

Violent conflicts and upheavals in the EU's eastern and southern neighbourhoods, new hybrid threats and terrorist attacks have strengthened the willingness in politics and society to intensify cooperation on European foreign, security and defence policies. This is the main assumption of the HRVP's first yearly implementation report of the EUGS in June 2017. The Rome Declaration issued by the European Council in March 2017 also makes it clear that the security of the citizens and territory of the EU is supported by politics and by a majority of EU citizens as a new integration narrative. This also means the EU wants to find a new purpose in a 'Europe of Security'. Federica Mogherini, EU High Representative for Foreign Affairs and Security Policy, and Jyrki Katainen, Vice-President of the European Commission, responsible for employment, growth, investment and competitiveness, both support a deepening of security policy. In January 2017, they made a case for expanding the EU into a real defence union not limited to the EU-27. They claimed that external measures and close cooperation with NATO could only improve the security of the Union. The new 'Europe of Security' is based on three major projects of current European policy: a security union, a defence union and intensive cooperation between the EU and NATO. All three are connected and have an important common reference point in European

Dr. Annegret Bendiek is a Senior Associate in SWP's EU/Europe Division

cybersecurity. The May 2017 attack on more than 200,000 computer systems in more than 150 countries has opened our eyes to the fact that strictly separating internal and external security is problematic in protecting critical infrastructure. Political activism in all areas of security and defence policy, as shown in the current implementation of the EU's Global Strategy (EUGS) since July 2016, has been spurred on by the perceived need to conceptualize a 'Europe of Security'.

Implementation of the EU Global Strategy (EUGS)

The imminent departure of the UK from the EU and Donald Trump's unpredictability as President of the United States are the main motives for the EU to seriously address its discussed but undefined goal of 'strategic autonomy' in the EUGS from July 2016. According to Trump and his government, most European states do not do enough for their security. Given the meagre success of European transformation efforts in its neighbouring countries, the EU is now trying, with the help of the EUGS, to make its citizens aware of the added value the Union can contribute to security issues. In order to ensure the security of its citizens and the territory of the EU, the following priorities were stipulated in November 2016: "(a) responding to external conflicts and crises, (b) building the capacities of partners, and (c) protecting the Union and its citizens". The Union is to develop greater resilience, i.e. have the capability to respond better to terrorist attacks, changes in cyberspace and hybrid threats. In order to achieve these aspirations, the EU will employ an integrated approach, that is the coherent use of military, civilian and economic instruments and closer networking of internal and external security. In August 2016, the Weimar Triangle states even suggested creating an independent form of the European Council to deal exclusively with questions of internal and external security. In November 2016, the German Minister of Defence advocated the long-term goal of a European security and defence union. The defence and security unions, however, would formally be separate from each other. The security union project is an initiative that has been largely promoted by the Commission and is primarily concerned with issues of internal and judicial policy. In contrast, the defence union is a political project devised by foreign and defence ministers. Cybersecurity policy breaks through this line of formal separation. It forms an interface between the major projects of internal and external security, as well as of internal, external and defence policy in the European multilevel system. It is, therefore, a focal point for new challenges associated with establishing the security and defence unions.

Political initiatives

The idea of a security and defence union is not new, but in the past it was mainly concerned with the external dimension of security. As early as 2002, the foreign ministers of Germany and France, Joschka Fischer and Dominique de Villepin, announced that the European Security and Defence Policy (ESDP) was to be developed into a security and defence organization. Since the summer of 2016, Germany and France have not only been arguing the case for closer cooperation on defence policy but also for internal security. Both countries are committed to a "Europe of different speeds". They want to focus more closely on flexible integration procedures, such as enhanced cooperation (Article 20(1) TEU), permanent structured cooperation (Article 42(6) and Article 46 TEU) and constructive abstentions (Article 31 TEU). European security is already variously organized along functional and regional lines. Not all Member States formally participate in either internal security policy or defence policy. The UK, Ireland and Denmark make use of their opt-out clauses on domestic and judicial policy. In addition, Denmark does not participate in the Common Security

and Defence Policy (CSDP). Also, not all EU Member States are in NATO. This applies to Finland, Ireland, Malta, Sweden, Cyprus and Austria.

Security union

The security union originated from the concept of an "Area of freedom, security and justice". It is implemented through the Tampere (1999-2004), Hague (2005-2009) and Stockholm (2010-2015) programmes and is enshrined in the Treaty of Lisbon (Article 3(2) TEU). The current Commission programme and restructuring of the Commission go a little further. From the outset, their objectives were to grow a stronger network of internal and external security and have internal and external policies. Following the terror attacks on French satirical magazine, Charlie Hebdo, the Commission presented its European Agenda for Security in April 2015. According to Commission President Juncker, organized crime, terrorism and cybercrime are cross-border challenges that represent "a common European responsibility" and create a deepening European cooperation within the framework of a European security agenda. One year later, in response to the terrorist attacks in Brussels in March 2016, the Commission announced its intention to establish a security union. Legally, this is essentially based on Article 67 TFEU, taking into account Article 4(2) TEU and Article 72 TFEU. Accordingly, the EU is "an area of freedom, security and justice", also known as the Schengen area. Commissioner, Julian King, who was newly appointed in September 2016, was entrusted with the task of implementing "Schengen security". He named his most important areas of action as, a) improving the legal framework for combatting terrorism, b) prevention and de-radicalization, c) improved exchange of information between Member States' authorities, d) the setting up of databases and their interoperability, e) protection of borders and f) better protection of critical infrastructures. Seven progress reports have been submitted for implementation to date. Among other things, a terrorist attack centre was set up at the European Police Office (Europol), arms legislation has been tightened and an antiterrorism directive and a data protection directive for electronic communication (ePrivacy Directive) have been issued. Police authorities in Europe are increasingly using data from different sources for their own evaluation and investigation activities. As a result, they have to cope with huge amounts of cross-border data and forensically examine them. In future, Europol will play an increasingly important role in the transmission of personal data. So far, Europol has concluded operational agreements to cooperate with the US, Canada, Norway, Switzerland and Australia. At the state and EU level, information technology will need bundled management. In May 2017 the Commission set out a new approach on interoperability of information systems.

Defence union

In its report on future EU military cooperation from October 2016, the European Parliament called for a newly created defence union to facilitate closer interlocking of national troops and to transform battlegroups, in existence since 2007 but never deployed, into standing units. In addition, Member States are to work together more intensively on the procurement of armaments which currently account for around 80 percent of solely national markets. According to the Commission, this practice generates annual costs of up to 100 billion euros. During his speech on the State of the Union in September 2016 and repeated in his speech on the defence union in June 2017, Commission President Juncker urged Member States to more closely coordinate their defence efforts. At the end of November 2016, the Commission presented its European Defence Action Plan (EDAP). The objectives contained in it go far beyond the headline goals agreed in 2008. It also states that it should be able to lead ten civilian and five military operations simultaneously and that a European Military Planning and

Conduct Capability (MPCC) be set up by June 2017. The predominantly political declarations of Member States to date are to become more legally binding. At the end of November 2016, the Commission presented plans for a European Defence Fund to promote joint investment in research and development which was launched in June 2017. Firstly, the fund will promote joint research on defence technologies, such as electronics, meta materials, encrypted software and robotics. The Commission has set aside 25 million euros for these technologies in 2017 and a further 90 million euros by the end of 2019. In 2018, the Commission will propose a dedicated EU defence research programme with an estimated annual budget of 500 million euros.

The multiannual financial framework of the EU after 2020 is to include a defence research programme worth around 500 million euros per annum. Secondly, joint armament procurement should be made easier for encrypted software or helicopters. A more substantial programme will be prepared for post-2020, with an estimated annual budget of one billion euros. The programme will leverage national financing with an expected multiplying effect of five. This should save five billion euros annually. It could, therefore, generate a total investment in defence capability development of five billion euros per year after 2020 according to the Commission communication. To achieve this, the Commission wants to support the European Structural and Investment Funds and the European Investment Bank (EIB) to finance the development of dual-use goods and technologies. Furthermore, general directives on the awarding of public contracts in the defence and security sector are to be extended. This should promote cross-border cooperation and advance the development of common industry standards.

Attention is being increasingly focused on aspects of dual use. A series of current projects by the European Defence Agency (EDA) deal with the question of how research findings can be applied equally to internal and external security. The first two research assignments were awarded to unmanned aviation systems and mobile reconnaissance robots for urban warfare. A third consortium was commissioned to develop an autonomous monitoring platform for both external and internal security. Autonomous reconnaissance systems, such as drones and sensors, are to be fitted with lasers and jamming transmitters in a 'swarm' system (EuroSWARM) and be placed under central command. The EDA believes the technology will be particularly important for border control and surveillance security.

EU-NATO cooperation

European security is not only a matter of improving cooperation on internal and external security but it is also a key action area within NATO. According to a framework agreement from March 2003 (Berlin Plus), the EU is allowed to make use of NATO resources and capabilities in military operations. Joint declarations by both organizations in July and December 2016 also reflect the Global Strategy's guiding principle that the Union's territory can only be effectively defended through cooperation between the EU and NATO. As a result, 42 measures were adopted to accelerate intensified cooperation in seven fields of action agreed at the Warsaw Summit in July 2016. These include defending against hybrid threats, early warning and situation on the ground, parallel operations in identical areas, cybersecurity and defence, interoperable capabilities, defence industry and research as well as exercises to strengthen the resilience of EU and NATO partners. The progress report of June 2017 on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 states that ten out of the 42 proposals are linked to the fight against hybrid threats. EU and NATO, along with Member States and Allies, are willing to contribute to and participate in the activities of the European Centre of Excellence

for Countering Hybrid Threats set up in Helsinki. Most Member States are in favour of close coordination between NATO and EU armed forces. All measures in the fields of foreign, security and defence policy should also, therefore, automatically strengthen NATO or at least complement its range of tasks. One example is the EU Hybrid Fusion Cell which was set up at the European External Action Service (EEAS). It is intended to bundle information from the security authorities of NATO and EU states, from EU institutions and partner countries. It is intended to act as an early warning system and to create a situation picture to defend against hybrid threats, such as cyber attacks. In addition, cooperation with Nato will also ensure that the CSDP is only directed externally, there is no provision for territorial defence and, contractually, there can be no deployments within the EU. Nonetheless, national defence is one of NATO's core tasks as a defence alliance.

Focus on cybersecurity

Cyber attacks on states and critical infrastructures have long been a reality. The quantity and quality of such attacks are growing steadily. Even the boundary between offensive and defensive orientation is fluid. If an actor has the ability to defend, he can also attack anywhere in the world. The difficulty of attributing these attacks, that is, the ability to clearly identify the perpetrator of an attack is an expression of the factual, political and technical limitlessness of cyberspace. The cyber and information space does not recognize national boundaries or institutional structures. Cybersecurity policy is a shared area of competence between Member States and the EU level. The NIS Directive "concerning measures to ensure a high common level of network and information security across the Union" came into force in July 2016. This has created a uniform European legal framework to provide national cybersecurity capacities from across the EU, to allow for more EU-level cooperation and minimum security requirements and to formulate reporting requirements for specific critical infrastructure services. Two new coordination mechanisms are being set up to put these uniform measures in place. A cooperation group is to support the strategic partnership and the exchange of information on cyber incidents between Member States, while the Computer Security Incident Response Team (CSIRT) is responsible for emergency support on the ground.

Cross-sectional task

EU cybersecurity policy is based not only on the NIS Directive but also on the 2013 Cybersecurity Strategy of the European Union and the 2015 Digital Single Market Strategy for Europe. It also builds on recent communications on the implementation of the European Security Agenda from 2015 and on defending against hybrid threats from 2016. Institutionally, cybersecurity at Council level is defined as a cross-sectional task and dealt with in the Horizontal Working Party on Cyber Issues (HWPCI). In crisis situations, cybersecurity also lies at the interface between civilian and military cooperation as well as internal and external security. If a major cyber incident were to occur, a whole series of EU institutions would cooperate with each other. These include the European Network and Information Security Agency (ENISA), the EU's Computer Emergency Response Team (CERT-EU), Europol's European Cybercrime Centre (EC3), the EU's Judicial Cooperation Unit, Eurojust, the EU Hybrid Fusion Cell, the EU Intelligence and Situation Centre (INTCEN) at the European External Action Service (EEAS) and the European Defence Agency (EDA). Just like the still-valid Cybersecurity Strategy, the future strategy will apply across all policy fields. The existing strategy contains five fields of action: Increasing resilience, combatting cyber crime, establishing a cyber defence, developing industrial and technical resources

and, finally, developing a global strategy for cyberspace. While European cooperation in the fight against cybercrime has already been able to boast successful investigations by Europol, the foreign cyber and defence policy so far remains the subject of well-intentioned declarations of intent.

Cyber defence

The EU Cyber Defence Policy Framework from November 2014 encourages EU Member States to review their cyber defence capabilities for the CSDP and ensure they are complying with their alliance commitments. The EU Military Staff has also called for better protection against cyber attacks on EU-led operations and missions. Cooperation between the EU and NATO on cybersecurity and defence, which has intensified since 2015, was formalized in the Warsaw Declaration in July 2016 and underpinned by specific implementation proposals made at the joint meeting of the Foreign Ministers of the EU and NATO countries in December 2016. In November 2016, the European Parliament made a strong commitment to deepen cooperation on cyber defence. It called on Member States to develop the necessary skills to achieve this in partnership with the EDA and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The aim is for the EDA to create synergies between NATO and EU capability developments. Projects for cyber defence include the Collaboration Database (CoDaBa) and the Capability Development Plan (CDP). Projects on cooperation between the EU and NATO include early warning capabilities for headquarters and a multi-agent system for Advanced Persistent Threat (APT) detection (MASFAD).

The ongoing review of the European Cybersecurity Strategy will have to take account of all these initiatives in internal and external security as well as data security developments in the digital internal market. High expectations have been placed on the upcoming Estonian Council Presidency. It is hoped that, among other things, it will finalize the digital single market and increase the legal force of cybersecurity. Estonia is seen as a pioneer in the single market and, at the same time, it wants to further develop European cyber foreign and defence policy in close cooperation with NATO. All this points in the right direction, since Europe, with the CFSP, the EEAS and the High Representative for Foreign and Security Policy, is named as the level at which Member State security and defence is to be developed.

Elements for a White Paper

For the Estonian Council Presidency in 2017, much will depend on the added value that Europe can provide on issues of digitalization, the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP). The final phase of the reflection process on the Commission's White Paper on the future of the EU will also take place during Estonia's Presidency. In June 2017, the Commission presented a longer-term reflection paper setting out possible scenarios for the future of EU defence. The Council Presidency will not deal with any fundamental issues of setting EU foreign and security policy which, as some politicians have called for, should be included in a European White Paper on Security and Defence. The aim of a 'Europe of Security' can certainly be seen as ambivalent. Should the security and defence unions actually develop into new core elements of the integration process, this could lead to a normative shift in the Union, away from the cosmopolitan demands of market integration and more towards a protectionist integration project. This Europe of security and defence should avoid a return to its old confrontational patterns, security dilemmas and an arms race, especially in cybersecurity. The necessary process of formulating a European White Paper on Security and Defence should, therefore, be supported by four main elements which focus on measures aimed at building trust and security.

1. The EU's pursuit of 'strategic autonomy' is a high and, at first glance, appealing aspiration. However, it contradicts the idea of an increasingly interwoven and interdependent world in which conflicts are not one-sided ('strategically autonomous'), but are resolved through dialogue and cooperation. It is, therefore, necessary to clarify what the term means for the EU's relationship with NATO. In principle, the idea of strategic autonomy is in competition with the aim of consolidating the European and US pillars of Western security policy. It is, therefore, necessary to oppose all the demands from science and politics for the US to withdraw from Europe or for Europe to create its own nuclear umbrella. Instead, the nexus between the North American and European pillars of NATO should be strengthened. Furthermore, additional common armaments projects would have to be considered. The goal should not be strategic autonomy but strategic interdependence.

2. If the EU and NATO want to cooperate even more intensively with each other in future, both sides must agree on what triggers the right for 'digital self-defence'. This includes a joint response to the question whether a serious attack on critical infrastructures should also allow 'offensive defence', i.e. an immediate military response. Attacks on critical infrastructures and the systematic use of security gaps by private actors also present policy-makers with the problem of how defence mechanisms at national and European levels can be simultaneously coordinated and what role should diplomacy and the military play here. In its White Paper 2016 on German Security Policy and the Future of the Bundeswehr, the Federal Government warned that terrorist organizations used "social media and digital communication to generate resources, attract supporters, spread propaganda, and plan attacks". Increasingly, they are able to use cyber capabilities to attack targets or use chemicals in assassination attempts. Even the use of biological and radioactive substances cannot be completely ruled out in future.

How would the EU in question state react? What forms of action are permitted under the common defence commitment? It is often very difficult to identify the perpetrators of cyber attacks. This makes it very difficult to legally assess the extent to which it is advisable to deploy political, legal, intelligence, police and/or military resources. In the event of a disaster or an attack, the solidarity clause (Article 222 TFEU) and the assistance clause (Article 42(7) TEU) permits direct assistance by Member States. The solidarity clause ensures that all stakeholders at national and EU level work together to respond quickly, effectively and uniformly to a terrorist attack and a natural or manmade disaster. The mutual assistance clause contains a duty to assist another Member State should it be subjected to an armed attack on its territory. Except in defence of their own country, German soldiers may not be deployed abroad unless it is expressly stipulated in Germany's Basic Law (Grundgesetz). Both the security authorities themselves and the laws underpinning their work, such as the separation requirement and the options of deploying the Bundeswehr internally, must at least be critically examined.

3. The EU urgently needs the responsibility to establish resilient network and information security systems and this responsibility needs to be enshrined in a legal regulation. To date, the European Network and Information Security Agency (ENISA) has been formally responsible for ensuring Member States are capable of responding rapidly in emergency situations and for effective EU-wide cooperation. However, far too many national critical infrastructures are still being secured at the national or private level. The exchange of information on cyber risks is not only weak between the EU and its Member States but also between the European agencies Europol, Eurojust, EDA and ENISA. The responsible Directorates-General only work to-

gether to a limited degree and are often not given the necessary information by Member States to establish a Europe-wide security network. Reform of the EU's Cybersecurity Strategy also aims to further develop the role of the EEAS and civilian cyber diplomacy instruments, i.e. measures to build trust and security such as the Cyber Diplomacy Toolbox. At the Political and Security Committee (PSC) meeting in March 2017 the EEAS/Commission services presented a joint issues paper on a joint EU diplomatic response to cyber operations ("Cyber toolbox"). The latter was welcomed by delegations as well as its suggested follow up in the Horizontal Working Party on Cyber Issues (HWPCI). Based on this list of sanctions, the EU can take political, financial and legal action to respond to those cyber attacks that are legally below the threshold of an armed conflict. Progress has certainly been made on cybersecurity in recent years. This applies to technical attribution, issues surrounding international law and trust-building measures in the United Nations Group of Governmental Experts (GGE), the OSCE and the G20.

4. Trust is a scarce resource in international relations. In order to generate more trust in information and communication technologies, additional investment is needed in technology, research, development and innovation. In August 2016, the EU set aside 450 million euros for the Horizon 2020 Framework Programme for Research and Innovation and, therefore, for security research. Cybersecurity market actors, represented by the European Cybersecurity Organization (ECSO), are to invest around three times this figure by 2020. If it is true that 'digitization is the commercialization of research findings by economic enterprises' (Frankfurter Allgemeine Zeitung, August 2016), then calls for independent civilian security research will quickly fall on deaf ears. Non-governmental organizations such as Digital Forensic Research Lab and Big Brother Watch conduct important civic investigative work. Critical security research is a necessary condition for establishing and maintaining societal and democratic acceptance of a 'Europe of Security'. National parliaments and the European Parliament should ensure that overcoming Europe's crises and setting up both a security union and a defence union do not come at the expense of liberal values. Nevertheless, one major challenge here will be to guarantee the priority of diplomacy over security and military policy, and to counteract any excessive securitization.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761

Translation by Martin Haynes

(English version of SWP-Aktuell 37/2017)