The European Security and Defence Union

Cybersecurity and global politics

How to protect our vulnerable societies in unpredictable times

60 years after the Elysée Treaty – putting the French-German relations back on track

Interview with

François Delattre, Ambassador of France to Germany, Berlin

Dr Hans Dieter Lucas, Ambassador of Germany to France, Paris

TWO MISSIONS. ONE SOLUTION.

It's your time to cook. Start cooking fresh and varied meals for your mission with our mobile catering systems. Whether with single modules, on a trailer kitchen or in a kitchen container. Discover the whole range at **kaercher-futuretech.com.**

FUTURETECH

Kärcher Group

Europe facing the ultimate test?

Europe and the west have lost their balance. The war in Europe was the inducement to recognise that the world was experiencing a break with the past and that all over the world the cards are being reshuffled.
Inside the European Union (EU), in some states the temptation to emulate populist promises is increasing, in others we are witnessing the breaking of partnership rules to the point of the elimination of democratic principles. Nationalistic tendencies develop against common tasks, supply bottlenecks are everywhere the result of too voluntary dependence in the globalisation of the economy. Europe watches the surge in migration with no ready solutions.
On the outside we witness the struggle of the great powers for geopolitical and military dominance and placement in a "post-Occidental" world, which means nothing more than stopping the influence of the west, as Indian President Modi said at the opening of the G20 summit 2022 mid-November in Bali.
The EU faces the crucial question of how to deal with the Union's own European sovereignty; whether it gives up the intention as a community to play a decisive global role in politics in the 21st century or whether it wants to become a pawn between the US and the authoritarian Chinese regime in their quest for dominance.
While the US, despite a domestic political and social crisis, is already emerging as the winner of the crisis in terms of energy and autonomy in feeding its population, doubts remain about the status of Europe. Due to Putin's war in Ukraine, the ranks of the NATO countries have closed and the US is again a real leading power in NATO, which at the same time has hammered down new geopolitical pegs in Southeast Asia with the security guarantee for Taiwan. With the renewed solidarity of the Europeans in NATO, the United States has managed, without particularly pushing, to undermine the EU's efforts to acquire greater autonomy in security and defence. Europe appears to be prioritising its role as the dependent European pillar in NATO. And the fact is, that wherever Europe has previously interfered in complex crises, it has lost, not because it was too weak militarily, but because Europe has lost its diplomatic creativity in dealing with the US, which is today no longer the model it was until the middle of the 20th century.

photo: private, USphoto.com

Hartmut Bühl

In the meantime Europeans have recognised that the development of strategic autonomy means immense efforts and that ultimately cannot be achieved without reference to the US.
Europe does not seem to be able to find a common political line, but acts technically and abandons politics for cooperative strategies that can build up into dangerous north-south contradictions, as shown by the dispute in the Union on capping energy prices, where Germany and some partners from the north in particular have long campaigned against. Above all, how money is handled shows how heterogeneous north and south are. The financially sound north has opted to support its industry and households, while the indebted south, oriented to France, has opted to cap prices.
Such differences have so far been resolved by the Franco-German engine, which is currently sputtering, with the risk of the Union splitting "ideologically" into a north pillar led by Germany and a south pillar led by France.
It is therefore now important to remember what we have in common and to give priority again to collectivity and to suppress national egoism. Therefore, the Franco-German engine must be restarted to avoid damage to the Union.

IMPRESSUM: The European – Security and Defence Union

Headquarters: International Consulting
6, Rue du Château, F 28260 Berchères-sur-Vesgre (FR)
E-Mail: hartmut.buehl@orange.fr
Publisher and Editor in Chief: Hartmut Bühl, Berchères-sur-Vesgre (FR)
Phone: +49/172 32 82 319
E-Mail: hartmut.buehl@orange.fr
Deputy Editor-in-Chief: Nannette Cazaubon, Paris (FR)
E-Mail: nannette.cazaubon@magazine-the-european.com

Editorial Assistant: Céline Angelov, Linz a. Rhein (GE)
E-Mail: editorial.assistant.esdu@gmail.com
Translator: Miriam Newman-Tancredi, Strasbourg (FR) and London (GB)
Layout: Beate Dach, SpreeService, Berlin (GE)
Advertisement & Sales: Hartmut Bühl, Berchères-sur-Vesgre (FR)
Phone: +49/172 32 82 319
Print: Polyprint GmbH (GE)

THE EUROPEAN –
SECURITY AND DEFENCE UNION
Vol. No. 46

Content

©bluedesign, stock.adobe.com

photos cover: ©Blue Planet Studio, adobe.stock.com; © Ambassade de France en Allemagne / MU (left); Deutsche Botschaft Paris (right)

© SasinParaksa, stock.adobe.com

©Boris Trenkel

The European – Security and Defence Union is the winner of the 2011 European Award for Citizenship, Security and Defence, and was awarded in 2019 the Jury's Special Prize of the same competition.

Ukraine

Standing ovation in the European Parliament

(ed/Nils Cazaubon, Paris) On 9 February, the President of Ukraine **Volodymyr Zelenskyy** addressed the European Parliament during an extraordinary session in Brussels. He already addressed MEPs remotely, however this was his first official visit to the Parliament. He received a three-minute-long standing ovation from the deputies as soon as he entered the hemicycle. In his speech, President Zelenskyy stated that Russia is not only fighting Ukraine, but Europe and its values as a whole. He thanked everyone who helped in the fight against the invader and rescued Ukrainian refugees. Zelenskyy hopes for a future where Europe and Ukraine walk side by side, but this future requires peace and security. "These dreams will not be possible if we do not overcome this anti-European force trying to steal our Europe from us", he said. European Parliament President **Roberta Metsola** stated: "We understand that you are fighting not only for your values, but for ours."

photo: European Union, 2023 - source: EP

The same day, President Zelenskyy also took part in the special European Council to discuss Russia's aggression and the EU's role in helping Ukraine and its people. He previously visited London, where he spoke in presence of members of the House of Commons and House of Lords before meeting King Charles III, and Paris where he had dinner with French President Emmanuel Macron and German Chancellor Olaf Scholz.

Video https://bit.ly/3lJkccW

Crisis management

EU help for Turkey and Syria after the earthquake

(ed/Nils Cazaubon, Paris) On 8 February, President of the European Commission **Ursula von der Leyen** and Prime Minister of Sweden **Ulf Kristersson**, in coordination with the Turkish authorities, have announced their intention of hosting a donors' conference in March, aimed at raising funding from the international community to help the people of Turkey and Syria after the devastating magnitude 7.8 earthquake of 6 February.

Turkish rescuer in front of destroyed houses

photo: © Adobestock/Adin

The disaster that hit near the Turkish town of Gaziantep caused widespread destruction of buildings and infrastructure including schools and hospitals, roads, airport, ports, oil terminals, electricity lines, and water provision. More than 44,000 people lost their lives in this tragedy. The people affected in Syria are families that were already displaced from their homes, living in tents or partially destroyed buildings. In Turkey, those hit by the earthquake include many thousands of refugees from Syria and the communities that have hosted them. The survivors, exposed to severe winter storms, urgently need life-saving shelter and assistance.

The European Union Civil Protection Mechanism was activated immediately after the earthquake: 20 EU Member States and Albania, Montenegro and Serbia have offered 31 search and rescue teams and 5 medical teams, consisting in a total of over 1,500 rescuers and 100 search and rescue dogs.

EU Presidency

Sweden's priorities for the European Union

On 1 January Sweden took over the Presidency of the Council of the European Union (EU) for the first half of 2023. Security, competitiveness, green and energy transitions, democratic values and the rule of law are the Presidency's four priorities in a time of historic challenges for the Union and its Member States.

Security: The Swedish Presidency will prioritise continued economic and military support for Ukraine, as well as support for Ukraine's path towards the EU. Sweden promotes a robust European security and defence policy, in close cooperation with partners and common action to counter Russia's aggression towards Ukraine.

Competitiveness: Sweden will seek to anchor a concerted approach to European competitiveness at the top of the political agenda to provide the best possible conditions for a sound and open economy based on free competition, private investment and successful digitalisation.

Green & energy transitions: The Presidency will continue efforts to tackle high and volatile energy prices while addressing a long-term energy market reform. The global climate challenge requires a global response and Europe must lead by example, by delivering on ambitious climate goals.

Democratic values and the rule of law: As the EU is based on democratic values, paving the way for cohesion, individual freedoms, non-discrimination, increased economic output and global influence, upholding the principle of the rule of law and fundamental rights is an essential element of Sweden's EU Presidency.

Web www.sweden2023.eu

UNESCO Peace Prize

Angela Merkel awarded for her refugee policy

photo: ©Shutterstock/sewonboy

The award ceremony for the **Félix Houphouët-Boigny-UNESCO Peace Prize** took place on 8 February in Yamassoukro, Côte d'Ivoire. The prize was awarded by **Audrey Azoulay**, UNESCO's Director General, and **Alassane Ouattara**, President of the Republic of Côte d'Ivoire, to former German Federal Chancellor **Angela Merkel** for "her courageous decision in 2015 to welcome more than 1.2 million refugees, notably from Syria, Iraq, Afghanistan and Eritrea", as stated the jury. In her acceptance speech, Merkel said that "working resolutely and hard for peace is even more important than it has ever been."

Created in 1989, the Félix Houphouët-Boigny Peace Prize honours individuals, institutions or organisations that have made a significant contribution to the promotion, research, safeguarding or maintenance of peace.

The prize has already been awarded to 29 other personalities, including Nelson Mandela and Frederik W. De Klerk (1991), Yitzhak Rabin, Shimon Peres and Yasser Arafat (1993), Mary Robinson (2000), Luiz Inácio Lula da Silva (2008), Giuseppina Nicolini and SOS Méditerranée (2017).

International security

Clear words at the 2023 Munich Security Conference

A few days ahead of the one-year anniversary of Russia's invasion of Ukraine, the 59th Munich Security Conference (MSC) took place from 17 to 19 February. The war in Ukraine dominated the international security event which gathered 450 international leaders and experts.

NATO Secretary General **Jens Stoltenberg** said that since there was no indication that Vladimir Putin has changed his ambitions, it is essential to "give Ukraine what it needs to win and survive as an independent sovereign nation in Europe". He warned that "if Putin wins in Ukraine, the message for him and other authoritarian leaders will be that they can use force to get what they want". The President of the European Commission **Ursula von der Leyen** and UK Prime Minister **Rishi Sunak** issued a joint statement saying that they agree on the importance of giving Ukraine the military momentum it needs to secure victory against tyranny. They also agreed that the European Union's and United Kingdom's efforts to train Ukrainian troops will make a real difference on the battlefield.

US Vice-President **Kamala Harris** formally accused Russia of committing massive human rights violations in the war in Ukraine, such as murdering, raping and kidnapping Ukrainian children. The MSC was also attended by the US Secretary of State **Antony Blinken** who accused China of failing to criticise Russia over its actions in Ukraine, while the Chinese foreign minister **Wang Yi** responded that America was prolonging the conflict by supplying weapons to Ukraine.

Web https://securityconference.org/en/

books & publications

Hybrid Warfare: Future and Technologies

by Ralph Thiele, Edition ZfAS / Springer VS, November 2021

Review by Harald Kujat, General (ret), Berlin

Emerging and disruptive technologies make it possible to initiate hybrid warfare with the aim of achieving already decisive advantages over an adversary before military combat operations of open war have started. They also create the necessary prerequisites to achieve comprehensive situational awareness and information superiority. From the targeted use of cyber and information technologies to deceive and confuse, to the elimination of the opposing command and information systems, the opponent can be weakened in the initial phase of a war to such an extent that the following military measures can be carried out with significantly lower risk and higher chances of success. Robotics, artificial intelligence, autonomous systems and hypersonic weapon systems will be decisive in high-intensity military conflicts of the future.

With his book "Hybrid Warfare – Future and Technologies", Ralph Thiele, an internationally recognised and valued expert in security and strategy has created a standard work on hybrid warfare. It is comprehensive in showing how political rivalries and conflicts will be carried out in the future using a wide range of emerging and disruptive technologies.

The author also outlines how open societies, and especially western democracies, can protect and actively defend themselves against hybrid attacks. The European Union and NATO should take up these proposals as soon as possible.

For Europe, this is a decisive prerequisite for a policy of political, economic and military self-assertion in the new power arithmetic of the global rivalry between the great powers.

Last update 22 February 2023

In the Spotlight

+++ Interview +++

Visit to Paris by the President of Ukraine, 8 February 2023. From left to right: Ukrainian President Volodymyr Zelenskyy, French President Emmanuel Macron and German Chancellor Olaf Scholz at the Elysée Palace

photo: Bundesregierung/Steffen Kugler

60 years after the Elysée Treaty

Putting the French-German relations back on track

Interview with François Delattre, Ambassador of France to Germany, Berlin and Dr Hans Dieter Lucas, Ambassador of Germany to France, Paris

The European: *Excellencies, I am honoured that both of you have accepted this conversation. 22 January 2023 marked the 60th anniversary of the signing of the Franco-German Elysée Treaty in Paris. What did the treaty mean to your respective nations at the time, and what is its significance for them today?*

François Delattre: The Elysée Treaty is a turning point in European history. By signing the treaty in 1963, Charles de Gaulle and Konrad Adenauer had the political courage to turn two long-time enemies into two of the closest nations and put their cooperation at the service of the European integration process. France and Germany decided to engage in a path of reconciliation that arguably has little precedent in history, with a special focus on youth, which has led to 10 million young people going on exchanges between the two countries.

The European: *And there have been further important initiatives since then.*

François Delattre: Yes, since then, we have deepened and structured the Franco-German relationship through the Aachen Treaty in 2019 and the establishment of countless channels of consultation designed to produce convergence between the two countries and to create what I would call a Franco-German reflex. I don't think there are two other countries in the world that are linked by such a dense and structured relationship in all areas. The other characteristic of the Franco-German relationship is that it is placed explicitly at the service of the European Union (EU). And in fact almost all of the major European initiatives, from the establishment of the single market to the creation of the euro and the recovery plan launched during the pandemic, have a strong Franco-German component – which obviously takes nothing away from the crucial role of the other EU Member States.

The European: *Ambassador Lucas, would you agree with Ambassador Delattre on the importance of the Elysée Treaty for Europe?*

Hans Dieter Lucas: 60 years ago, the signing of the Elysée Treaty symbolised the reconciliation between France and Germany after the two world wars. This reconciliation is a central pillar of the European peace project, but at the same time the Elysée Treaty expressed the will to build the future together. It opened an era of intense unprecedented cooperation in all areas. History shows that the Franco-German "motor" is not sufficient, but certainly indispensable for progress of the European construction. This is particularly true in these times of multiple crisis. Europe is at crossroads – and Germany and France have a special responsibility in bringing it together.

The European: *For some time now, the media have been reporting that this binational motor is sputtering and that Franco-German relations will be weakened in the future by national egoism detrimental to the EU. What are the difficulties?*
François Delattre: The strength of the Franco-German partnership is that, from often very different starting positions, it produces convergences which in turn will serve to achieve a European consensus. The ability to overcome our differences through dialogue is our great strength. Moreover, France and Germany have a common reading on the Russian military aggression against Ukraine and on the consequences to be drawn from it for Europe and its sovereignty. In such a profoundly upset strategic context, you cannot go by the book, you have to get out of autopilot. This is the meaning of the "Zeitenwende" (epochal shift), put forward by German Chancellor Olaf Scholz. So we had to put all subjects back on the table and get back to work even harder, which is what we did on defence, energy, and industrial policy to take just a few examples.
As a result, the Franco-German partnership is back on the right track and the engine for Europe is running at full speed again. This is illustrated by the last French-German Ministers Council on 22 January and by the Paris meeting between the French President, the German Chancellor and Ukrainian President Volodymyr Zelenskyy on 8 February. This is good news for Europe as well as for the transatlantic partnership.

Hans Dieter Lucas: The close Franco-German partnership is based on our shared understanding that Europe can only be strong and peaceful if Germany and France work together. This is something that all successive French presidents and German chancellors have understood and valued since the signing of the Elysée Treaty. It is the shared will to find solutions to the pressing problems in Europe, despite the differences that sometimes exist between our two countries, that has distinguished our cooperation for over 60 years and

photo: © Ambassade de France en Allemagne / MU

"I don't think there are two other countries in the world that are linked by such a dense and structured relationship in all areas." Ambassador François Delattre

photo: Deutsche Botschaft Paris

"Europe is at crossroads – and Germany and France have a special responsibility in bringing it together" Ambassador Hans Dieter Lucas

made it so important. As Ambassador Delattre said, the recent German-French Council of Ministers clearly showed that we agree on many issues, in particular to actively contribute to making Europe stronger and more "sovereign" in every aspect. This becomes all the more evident in times of crisis: I need only recall the Covid-19 pandemic, during which Germany and France jointly paved the way for the historic EU recovery fund. The same applies to the Russian aggression in Ukraine. The unprecedented sanctions against Russia were coordinated in the closest consultation between Berlin and Paris, as well as with our European partner countries. One could even say that the Franco-German partnership not only weathers crises as you said, but it thrives in times of crisis, when its importance becomes so acutely clear to everyone.

The European: *Excellencies, let me turn to current burning political issues. Firstly energy: both nations have become dependent on their sources of energy, with serious consequences: Germany's unwise dependence on Russia; the French dependence on nuclear energy plants, with their worrying technical failings. Is there a common future?*
Hans Dieter Lucas: Germany has ended its energy supply from Russia concerning coal, gas and oil in record time. Just two months ago France and Germany recalled in a political declaration their commitment to achieving climate neutrality by 2050 and 2045, respectively, and their determination to reduce their dependence on fossil fuels. In this context, they underlined the need to organise the transition to a decarbonised energy supply, while respecting the principle of technological neutrality with regard to the national choices of energy mix. For Germany it is clear: we will achieve our climate goals by massively expanding renewable energies in the years to come. As far as nuclear energy is concerned, our differences are well known.

The European: *Ambassador Delattre, there is an understanding to achieve the objective of climate neutrality as Ambassador Lucas*

→ *Continued on page 10*

In the Spotlight

+++ Interview +++

mentioned. But there is obviously no common French-German approach to achieve the shared objectives.

François Delattre: Concerning energy, it is obvious that our starting points, and energy mixes are very different. That is why we must create the conditions for convergence around the objectives that unite us, starting with the security of energy supplies in Europe and the rapid reduction of our CO_2 emissions. That's exactly what we are doing right now. I'm not saying it's easy, but we'll get there because the political will is there.

From France's point of view, the best way to meet these two objectives and move away from fossil fuels is to move forward from a good balance between nuclear energy and renewables. Many of our European partners are on this line and for instance view nuclear energy as a key asset to produce carbon free hydrogen, of which we will collectively need significant amounts. Here too France and Germany, together with their partners, must respect their differences and build on their common objectives, carbon neutrality in particular.

The European: *In the new geopolitical configuration in which Russia is extensively isolated and China increasingly so, is there an opportunity to relocate entire branches of industry? Could Germany and France play a pioneering role for Europe by proposing joint solutions for a new European industrial policy?*

Hans Dieter Lucas: I think there is no industry that can be relocated from Russia to Europe. Regarding China, we seek cooperation with China wherever possible and when it is in our interest. We want a rules-based relationship with China. At the same time China is not only a partner but also a competitor and systemic rival. That is why we are reassessing the risks of doing business with China. We need to diversify. Regarding European industrial policy: Germany and France agree on the necessity for a strong European industrial policy enhancing Europe's competitiveness. In November, Bruno Le Maire and Robert Habeck, our ministers for economy, published a joint statement, saying "We call for a renewed impetus in European industrial policy". That is what we are working on.

The European: *Ambassador Delattre, could you define the sectors where we can enhance competitiveness along the new roadmap the European Commission published on 1 February?*

François Delattre: Indeed, much is at stake to strengthen Europe's industrial attractiveness and competitiveness and make sure that we approach in the best possible conditions the three technological revolutions that will largely determine our future: the revolution of energy and sustainable development, the revolution of life sciences and genetics, and the digital revolution with its extensions into Big Data, artificial intelligence, the cloud, the Internet of Things and quantum technologies, to name just a few. France and Germany certainly have an important role to play in this regard, in conjunction with their European partners.

The European: *On 7 February, the French and German economy ministers travelled to Washington to promote a Euro-American approach to the US Inflation Reduction Act (IRA). This seems to be a strong message of French-German unity at the service of Europe and the transatlantic partnership.*

François Delattre: We are indeed at a decisive turning point for the European industry. Our companies must adapt rapidly to the ecological and digital transitions while reducing their strategic dependencies and continuing to benefit from a level playing field. Our task is to give them the stable framework that will allow them to keep growing and contribute to Europe's prosperity and sovereignty. As a Franco-German team, we will build on the roadmap published recently by the Commission. We must build a genuine "made in Europe" strategy that will give Europe the means to decisively strengthen its attractiveness and competitiveness. Reducing our dependencies, on China particularly, is also central. It forces us to rethink our value chains and pursue a "de-risking" strategy in order to avoid a decoupling that would hurt Europe most. Germany and France have a converging strategy on this.

The European: *Finally, let me come to armaments cooperation. There have been many positive achievements in the past, but also a lot of tension. Large-scale cooperation projects are highly political and thus stir controversy if they fail. How can the two governments and their respective industries approach projects in the future?*

Hans Dieter Lucas: Armament cooperation is not a luxury but a necessity. Cooperative programmes, if successfully implemented and thought through from start to finish, offer many advantages. We are committed to the goal of a strong European Defence Technological and Industrial Base (EDTIB) and German-French cooperation is essential for strengthening European military capabilities. It is evident that large projects like the Future Combat Aircraft System (FCAS) or the Main Ground Combat System (MGCS) cannot be handled by one nation alone. It goes without saying that these major projects are challenging, but what finally counts is our shared ambition to make them happen. Of course, that requires both sides to take each other's strengths and weaknesses into account – this is the core of every genuine partnership.

François Delattre: Strengthening European cooperation in the field of defence industries is a key component of European geopolitical, industrial and technological sovereignty. This requires taking into account our common long-term interests, beyond short-term constraints. In this area, the recent announcement of an agreement between France, Germany and Spain and their manufacturers on the first phase of the combat aircraft of the FCAS marks an important step forward.

The European: *Excellencies, I thank you for this conversation.*

The interview was led by Hartmut Bühl.

COMMENTARY

The war in Ukraine at a turning point?

by Hartmut Bühl, Publisher, Paris

Has the war in Ukraine reached a turning point with the announcement that the west will deliver "Leopard2" main battle tanks to Ukraine, after such a long time of hesitation from Germany to send them and authorise their re-export from partner countries?

First of all, there is the courage and bravery of the Ukrainian people, inspired by a President who is not afraid to point out that his country is a bulwark against despotism and imperialism. And who doesn't shy away from telling western statesmen what weapons his country needs to win the war, whatever that means. Will Zelenskyy be able to convince NATO to be as hawkish as he would like it to be to crush the Russian military machine deployed against his country?

Secondly, the war in Ukraine is not only a war between Russia and Ukraine, but also a war over the geostrategic interests of the United States to achieve supremacy over Russia and prepare to resist China's policy of enlarging its sphere of influence.

Thirdly, there is Europe, which, contrary to expectations, has united behind Ukraine. Immediately after the Russian invasion, the European Union imposed sanctions on Moscow and began supplying arms to strengthen the Ukrainian armed forces.

Fourthly, there is Germany, the economic giant at the heart of Europe with no ambition to play a leading military role. However, the invasion of Ukraine has triggered a real paradigm shift in Germany. Chancellor Scholz spoke of a historical turning point ("Zeitenwende") just a few days after the Russian invasion and announced a special fund of €100bn for the neglected German armed forces. And then came a true psychological breakthrough given Germany's past: the German Parliament lifted the ban on the export of military equipment to crisis areas. But the population is still influenced by the deeply held belief that "nobody should blame Germans for being responsible for another war".

The other belief, "never alone", voiced by Chancellor Scholz in the debate about the delivery of tanks, has the same roots, the weight of history, but also reveals a lack of confidence in Germany's own sovereignty and the fear of being responsible for a possible escalation. And in any decision, the logic of "only together with allies and not without America" prevails.

These ties to America as Germany's nuclear protective power has nothing to do with Germany's neglect or even betrayal of a common European defence, as its European partners often accuse it of, when they complain of Germany's lack of geopolitical and geostrategic thinking. That isn't reason enough for blame: after the liberation from the Nazi regime, Germany was divided into two. Neither state was soverein and western Germany' forces were completely involved in forward defence. There was no need for strategic thinking contrary to the US, France and Great Britain with their maritime vocation and their geopolitical past.

Finally, there is the question of how the war in Ukraine will end. First of all, it will be necessary to define what is meant by "Ukraine must not lose" or "Ukraine must win the war". Who will decide? Which format for negotiations could be created? Another version of the Budapest Memorandum with Great Britain, Russia and the US? Certainly not! A new format under the aegis of China?

Whatever the format of negotiations will be, it is crucial to keep in mind that whatever peace deal is eventually struck, it must not contain the seeds of the next war.

photo: © pronoia, stock.adobe.com

In the Spotlight

+++ Middle East +++

Transformation processes in the Middle East

Turkey's new role and the Russia-Ukraine war

by Gerhard Arnold, Publisher and Middle East correspondent to this magazine, Würzburg

Since the start of the Russia-Ukraine war on 24 February 2022, the Turkish President Recep Tayyip Erdoğan has had an astonishing presence on the international and regional political stage. If one wants to adequately understand the Turkish leader's increase in foreign policy prestige as a result of the war in Ukraine, one must carefully consider the regional political environment in the Middle East, his relationship with NATO and western European countries, and his policy initiatives prior to the war.

Erdoğan – the troublemaker

Since the failed coup by small parts of the Turkish military in the night of 15 to 16 July 2016, Turkey's relationship with Europe and the United States (US) has continued to deteriorate. Head of state Erdoğan unsuccessfully demanded that the US extradite former comrade-in-arms Gülen, allegedly a driver of the coup, and increasingly expanded his country into a totalitarian police state, dismantling democracy, freedom of expression, etc. In June 2019, Erdoğan made it public that he had purchased advanced S-400 air defence missiles from Russia, further angering the US.

Relations with the Arab world also deteriorated as a result of Turkey's ongoing islamisation and Erdoğan's readily apparent efforts to build a neo-Ottoman hegemonic policy. Against the interests of the conservative Gulf states, he supported the Arab revolts in 2011, but also the Islamist Muslim Brotherhood, a terrorist organisation in the eyes of Gulf neighbours. His military intervention in Libya in January 2020 in favour of the official government led to direct confrontation with key Arab states. By 2020, Turkey's reputation was at an all-time low in western Europe, the US, and key Arab states.

> "Erdoğan will take advantage of the discernible Russian loss of power to further advance Turkey's hegemonic policy."

Turkey's political reorientation

It was not the Russia-Ukraine war, but developments the year before that led to a political reorientation of Erdoğan's foreign policy toward the Arab world. The main reason was the growing economic and financial problems at home, combined with very high inflation. This limited his domestic scope for further aggressive hegemonic policies.

The change of president in the US from Trump to Joe Biden in January 2021 led to a strategic reorientation in the United Arab Emirates (UAE) and Saudi Arabia, a consequence of the announced American disengagement in the Middle East.

In search of new strategic partners, they were open to Turkey's advances, but expected it to end ties with the Muslim Brotherhood. Turkey, for its part, was primarily interested in new sources of money, in large financial investments to boost its own economy. The UAE offered itself. Bilateral visits by government delegations, state visits and personal meetings at the presidential level in 2021 and 2022 slowly

thawed the icy relations with Egypt, the UAE and even Saudi Arabia. Normalisation was also achieved with Israel.
These developments have noticeably weakened, though not overcome, Turkey's years of political confrontation with key Arab countries. The numerous and bloody conflict dynamics in the Middle Eastern crisis region and North Africa have not been changed by Turkey's new regional policy.

The Ukraine war – a gain in prestige for Erdoğan

The war in Ukraine, which began with a Russian attack, affected relations with Arab states, as well as with other NATO countries.
Several Arab countries were affected by the consequences of the war very quickly and, in some cases, severely, because the previously secure supply of Ukrainian grain was interrupted. It primarily affected Egypt, but also Jordan, Lebanon and Morocco, as well as many African and Asian countries.
Erdoğan, supported by the UN Secretary General, managed to find an export agreement for grain products in negotiations with Russia and Ukraine in July 2022. Slowly but steadily, shipments increased again. Turkey's geographic location at the southern exit of the Black Sea gave it control of the sea route through the Bosporus and the Dardanelles, which increased its international political weight in the war. Erdoğan also succeeded in extending the duration of the grains agreement beyond 19 November 2022, another diplomatic success of importance for Arab states.
For several years, Turkey has maintained close political and military relations with Ukraine, whereas political relations with Russia were very complicated on both sides, but respect for mutual interests allowed agreements and avoided confrontation. Economic cooperation is considerable, particularly through Russian tourists in Turkey and the large deliveries of Russian gas and oil. Since the beginning of the Russia-Ukraine war, the Turkish leader positioned himself as a political mediator between Ukraine and Russia. After two unsuccessful rounds of high-level talks in Istanbul and Ankara in March 2022, Erdoğan was involved in a prisoner exchange between Ukraine and Russia in September 2022.

New policies and old obsessions

The internationally acclaimed Turkish initiatives, which led above all to the resumption of important grain exports, strengthened Erdoğan's reputation at home and abroad. His policy to establish Turkey as a major neo-Ottoman regional power in its own right, no longer unilaterally fixated on the west or the United States was beginning to be successful. NATO also viewed Turkish mediation with some respect. Surprisingly, Erdoğan also sought to bear political mediation between the two states, in contrast to his previous unilateral political and military support for Azerbaijan in the conflict with Armenia.

In the shadow of international attention to the Ukraine war, Erdoğan has been able to pursue an old political obsession, the fight against Kurds in northern Syria and northern Iraq, driven by his fear that they will seek their own Kurdish state. The series of Turkish attacks on Syrian and Iraqi territory since 2016, in violation of international law, continued on 20 November 2022. Erdoğan ordered twelve airstrikes on Kurdish positions in north-eastern Syria, and in the weeks before that, almost daily sorties with combat drones. Erdoğan's ongoing conflict with the Kurds put additional strain on relations with NATO in 2022. hen Finland and Sweden applied for NATO membership on 18 May 2022, in light of Russia's attack on Ukraine, striving for quick admission, Turkey blocked the procedure, accusing Sweden in particular of not taking decisive action against Kurdish terrorists, but instead granting asylum to quite a few of them. But the Turkish demand to extradite them is hardly acceptable to Sweden from the point of view of the rule of law.

Pushing forward into the power vacuum

Erdoğan has been walking a risky tightrope between his loyalty to the alliance as a NATO member and his political relations with Russia since the beginning of the Ukraine war. His political mediation activities between Ukraine and Russia, especially the export agreement for grain from Ukraine, have significantly increased his international prestige. He has also been able to broaden his foreign policy scope in the Arab world, a process that began even before the Russia-Ukraine war. Head of state Erdoğan will take advantage of the already discernible Russian loss of power in the former states of the Soviet Union and in the Caucasus to push forward into the power vacuum there and further advance Turkey's hegemonic policy. Erdoğan's new policies also serve to bolster his domestic standing with voters in the run-up to Turkey's next presidential and parliamentary elections on 18 June 2023. But this calculation may not work out. The two massive earthquakes in south-eastern Turkey on 6 February 2023 have caused grief and despair among the population, but have also led to increasing criticism of the president's disaster management.

Gerhard Arnold

photo: private

is a German protestant theologian and publisher. Born in 1948, he served as minister in the Lutheran Church of Bavaria and was teacher of religion at a High School in Kitzingen from 1982- 2009. Mr Arnold published numerous monographs and essays in the field of contemporary church history on the themes and issues of ethics of peace and international security policy.

GUEST COMMENTARY

Franco-German relations – a tale of lost confidence and the need for new pragmatism

by Stefanie Buzmaniuk, Senior Research Fellow, Robert Schuman Foundation, Paris

For some months now, the message has been clear in France: the Franco-German couple needs a "couple's therapy". The need for more emotions and affirmative reactions from the German side is repeatedly expressed by the French. The German media, on the other hand, have far less reported on the Franco-German crisis; "couple's therapy" is rarely demanded, also because the word *couple* is perceived as a term that is too intimate for such a practical relationship. The Germans prefer the word *motor* (engine). Still, the German side does feel uneasy about its current relation with France, but first and foremost because France is understood as the country mainly pushing its own agenda on the European scene without considering German interests.

There seems to be a big misunderstanding. Both countries are disappointed in the other's attitude and have lost the appetite to negotiate. Even though grand symbolic statements were made on the occasion of the 60th anniversary of the Elysée Treaty, the Franco-German tandem is rusty on the level of European, bilateral and even local cooperation with difficult negotiations in the European Council, the Franco-German Council of Ministers being postponed, less and less young Germans speaking French and vice-versa.

This is not good news for the rest of Europe. Since the beginning of the creation of a united Europe with the Schuman Declaration in 1950, it had been obvious: without close cooperation between the two historically war-torn countries, Europe will not be able to move forward.

This is still the case. If France and Germany are not looking in the same direction, no consensus on a European level can be found. Of course, negotiations are always necessary to get there, because instinctively, France and Germany have different views on all sorts of priorities and policies. What is currently worrying, though, is that the most important disagreements exist in the political fields that matter the most at the moment: defence, energy, and economy. Negotiations on all these subjects are stalling.

The awareness of urgency and common interests has to be found again: in times when war is back on our continent, Europe needs a strong and united answer in order to be able to defend itself against hybrid, conventional, and even nuclear aggression. At the moment, when traditional energy supplies are rare and expensive and new and clean energy forms have to be found and financed, only a European approach can live up to the challenge. When inflation hits hard and the US puts Europe under pressure with its Inflation Reduction Act, mobilising $370bn in subsidies from 2023, no national answer will be sufficient in order to bring our economy back on its feet and ensure that it remains competitive.

Even though Franco-German relations have cooled down, they need to be rebuilt on all levels. This can only be done by finding mutual trust and confidence in each other's words again and by rediscovering interest in the other side's perspective. However, expectations need to be managed: on certain topics neither France nor Germany will move. NATO will remain the main building block of German defence and France will continue to push for a European approach. These two visions, though, are not mutually exclusive and currently both sides seem to have understood one part of the solution: NATO does remain essential for European defence as Russia is continuing its unjustified war against Ukraine, and building a stronger Europe which can defend itself and has a resilient and interoperable defence industry is indeed more vital than ever before.

The German and the French sides need to reckon with mutual differences, work with and around them in order to stay strong together and find new ways forward by combining their efforts. Common interests are nowadays plentiful, the road to reaching them must be taken with a newly found pragmatism.

Stefanie Buzmaniuk is Senior Research Fellow and Development Manager at the Robert Schuman Foundation where she previously held the position of Head of Publications. Furthermore, she is an external lecturer at the French business school ESSEC, teaching the course "European Kaleidoscope". She also worked as Research Assistant in the German-British think tank Convoco in London. Her research focus lies on the politics of European migration, the Franco-German relationship, and European identity.

MAIN TOPIC

Cybersecurity and global politics

Protecting the cyberspace has become a challenge for our highly connected societies. Massive attacks of disruption against governmental institutions and critical infrastructure can paralyse a whole country. The Russian cyber-offensive against Ukraine shows that digital strikes have become a fearsome tool in the global power play.

photos: ©metamorworks, stock.adobe.com

A high level of cooperation in cybersecurity is required for European societies to remain safe

Digital dependency has become all-pervasive

by Nick Watts, Vice-President EuroDefense UK, London

With the advent of a globalised and digitised world, the cyber threat has become all-pervasive. Unlike any other vector of warfare or terrorism, the cyber threat can reach into the lives of every citizen, and every business. To ensure that European civil society, as well as national security structures remains safe, a high level of co-operation is required. To do this, Europe can make use of its own cyber security standards, to help protect its citizens.

The IT realm is protected by civil and criminal law. The EU has competences in these areas – so regulations and directives can provide a necessary underpinning to safeguard the essential elements of a civic society. This includes Intellectual Property – which is highly prized by hostile states; the regulation of finance – which can be subverted by the use of 'dirty' money to finance criminal activity and arms trafficking; and data security – which can protect citizens from having their data stolen and misused to infiltrate sensitive web-sites.

> "The cyber threat can reach into the lives of every citizen, and every business."

As the EU develops competencies in the areas of defence and security, a strong 'home base' is essential to ensure that society can flourish, and to ensure that national defence and law enforcement structures are not compromised. Digital dependency has become all-pervasive. There is an opportunity for the EU – alongside international partners, to use its regulatory framework to require traders from third party countries to comply with its cyber security standards. Both sides benefit. The EU protects itself, and the trading partner gains the highest level of cybersecurity. To avoid claims of protectionism, the EU can offer to export its knowledge and best practice – a cyber version of the single market.

Introducing the cyber domain

In the modern era, the war of 1914-1918 was the first occasion where 'signals' intelligence played a significant role, from intercepting communications on the battlefield, to reading diplomatic cables. During the war of 1939-1945, the full panoply of electronic warfare was put to use; as well as 'signals' intelligence, code breaking, radar and jamming were widely employed by all sides. And as technology evolved during the Cold War, so did the realm of electronic warfare. The advent of the 'Fifth Domain' – Cyber emerged in 2010, from a fusion of electronic warfare and the widespread use of IT in the defence field.

The recognition of an IT risk led many governments to rapidly produce cybersecurity policies to protect their most essential defence and security systems. Only then did governments and security agencies realise that the cyber risk affected every element of modern society, with back doors into many sensitive areas unlocked. Notoriously, the revelations by Edward Snowden in 2013, that the US National Security Agency (NSA) and other agencies were intercepting the e-mails and telephone calls of foreign heads of state, made the wider public, and policy makers, aware of the cyber risk. The Snowden revelations sparked a debate on the balance between security and the freedom of the individual in a civic society.

Europe's response to growing cyber threats

The challenge for policy makers in the national security space, as well as in the commercial world, is to ensure that the stand-

Nick Watts

photo: private

is Vice-President of EuroDefense UK. He has been a policy advisor and freelance journalist in the defence and security sphere since 2001. He previously served in the British Army in west Germany and in a reserve armoured reconnaissance regiment.

ards they mandate are relevant. The process of law making in a democracy can be slow. The same applies to the military, where doctrines and tactics have to be revised and are now encompassed by the doctrine of 'fusion'. The "fusion doctrine" is where all sensors and systems can be linked together to produce information in real time.

The EU has increased its activities in the cyber domain, beginning in 2013 with a Cybersecurity Strategy. The Tallinn Digital Summit in September 2017 called on the EU to become a global leader in cyber security by 2025. On 12 March 2019 the European Parliament adopted the European Cybersecurity Act. This establishes an EU wide cybersecurity certification framework. It also gives a permanent basis to the EU Agency for Network and Information Security (ENISA). Previous legislative steps include the Network and Information Security (NIS) Directive, adopted in 2016 and the General Data Protection Regulation (GDPR), adopted across the EU by May 2018.

More recently, the Strategic Compass, published by the European Commission on 21 March 2022, refers to the cyber threat as part of the changing threat landscape and sets out several measures. Finally, on 16 January 2023 three cybersecurity-related legislative acts came into force: the NIS2 Directive, the Resilience of Critical Entities (RCE) Directive, and the Digital Operational Resilience for the Financial Sector (DORA) Regulation.

Developments following the invasion of Ukraine

It is too early to speak definitively of 'lessons learned', but some emerging themes are shaping the policy responses by national governments, security agencies and international organisations such as NATO and the EU. On 10 January 2023, a joint NATO-EU communique noted: "We have reached tangible results in countering hybrid and cyber threats, operational cooperation including maritime issues, military mobility, defence capabilities, defence industry and research, exercises, counter-terrorism, and capacity-building of partners." The significance of this is a recognition that cyber security is a shared responsibility and a vital necessity. Russia's use of its cyber capability, during this campaign has been less devastating than many commentators expected. However, Ukraine and the IT community began to understand the nature of these attacks. They were based on commercially available software, so they were dealt with.

There are multiple open source reports about assistance given to the Ukrainian government. Some of this assistance came from US Cyber Command, and some was provided by IT companies, following a 2015 attack on the power grid of Kyiv. These efforts were increased in autumn 2021 when the threat from Russia was assessed as having amplified. Of particular concern was the IT system for Ukrainian railways. This system has proven to be very resilient. After hostilities began, Russian cyber-attacks were mounted on border police, as well as national police computers. These attacks were dealt with via the use of hardware provided by Fortinet. Attempts at malware attacks were identified and reverse engineered by Microsoft engineers. The company reports that within three hours a software update was issued.

Best practice in the cyber domain

Modern societies are increasingly adopting digital methods of working in the commercial, governmental and national security fields. Governments are reliant on commercial IT vendors for much of their technical know how. A modern society, therefore, needs to adopt a "fusion doctrine" that embraces all aspects of its commercial and governmental sectors. The EU has an opportunity to export cybersecurity to its allies and partners, via its regulatory framework. Just as commercial companies wishing to trade in the Single Market must adopt EU standards, so there is an opportunity to reinforce the benefits of best practice in the cyber domain. For example in cyber the UK has expertise second to none in Europe. Therefore it is important that from its own defence and security, the EU enables UK input to its standards and the UK is not disadvantaged – from either a commercial or a security point of view – by being excluded.

The EU has developed a technical capability to come to the aid of Member States that suffer from cyber-attacks, via Cyber Emergency Response Teams (CERTs). In the same way, the EU can provide Information Assurance (IA) assistance, as well as CERT know-how to those who choose to do so.

photo: © Vitalii, stock.adobe.com

Technological progress and production capabilities cannot be conquered militarily

How cyber-attacks are influencing global politics

by Professor Dr Thomas Jäger, Chair of International Relations and Foreign Policy, Cologne University, Cologne

The international order is currently undergoing a geopolitical realignment. While the Unites States (US) and China are fixed as the two centres of the future world order, other powers are also striving for a place as world powers. But the prospects for Russia and the European Union (EU) are bleak for different reasons, and India will not be able to assume this role in the foreseeable future either.

In this regard, Russia's war against Ukraine, which was intended to usher in dominance over Europe, is acting as a catalyst in several directions in cyberspace. First, these capabilities have a major impact on the current war effort. Second, they illustrate the value of technological advances to a politically and economically dominant international position. Third, they redefine the gap with states with lesser cyber capabilities. Fourth, they describe the challenges for a new form of cooperative arms development – or its failure.

A new form of warfighting

Russia's war against Ukraine is often discussed in terms of analogies of the first world war: trenches, war of attrition, artillery skirmishes. But it could not have been fought by either side without intensive reconnaissance, the close networking of cyber capabilities with other weapons systems. One of Ukraine's advantages lies precisely in being more effective and efficient here, and therefore faster. The importance of the Starlink satellite service to warfare documents this, as it makes real-time warfare possible.

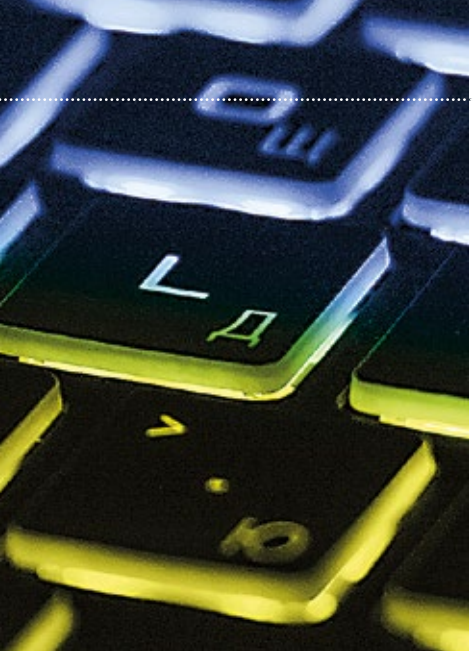
In addition, a total of 2,194 cyber-attacks were carried out by Russia in Ukraine in 2022 and 1,655 cyber-attacks on civilian infrastructure since the beginning of the war. Such cyber-attacks have also been registered in other states and campaigns of disinformation have been run by Russia. Throughout the west, companies are said to be weakened by blackmail and trade secrets are stolen. More significant than these current actions, however, is the question of who will have the most advanced capabilities in the future.

Reducing technological dependencies

In order to use the determining advantage for itself in the future, investments in semiconductor production are promoted. Thus, a parallel rivalry for the manufacturing capacities of semiconductors and microchips is being waged. Production capacity is being built in the US and EU to reduce dependence on Taiwan's TSMC and other companies production abroad. The US has launched a $52bn subsidy through the Chips Act for America 2022, which has since triggered $122bn in investment from TSMC, Intel and Samsung in the US. The EU is in the process of lining up $43bn in subsidies for semiconductor manufacturing in the EU. At the same time, the US has imposed trade restrictions on China to slow China's progress on semiconductor manufacturing. The Chinese government is already investing heavily and plans to implement another $143bn investment programme starting in 2025. The goal is technological self-sufficiency, after the US has repeatedly restricted the access of China's companies – for example, by imposing sanctions on Huawei. Chinese companies are currently far from the technological progress of the US or Taiwan. As things stand today, China will neither be able to meet the 70% semiconductor target through its own production by 2025, nor will it be able to match the technological developments of American and Taiwanese companies.

> "The availability of semiconductors and microchips has become a matter of national security, and technological progress in this field has become an imperative for superior weapons systems."

Even before the war, governments sought



to renationalise production of strategically important goods because of the pandemic and disrupted supply chains. Russia's war against Ukraine and China's threats against Taiwan's independence have accelerated this process. Production capacities and trade relations are being adapted to the new geopolitical situation. This is because the availability of semiconductors and microchips has become a matter of national security, and technological progress in this field has become an imperative for superior weapons systems. Therefore, it is not only a matter of being at the forefront of this technological progress, but also of preventing others from having these capabilities. Countering industrial espionage becomes a vital interest. This has implications for economic relations beyond the defence equipment itself.

A coordinated design of cyberspace

In addition to building the capabilities, their use must be analysed and designed. Cyberspace must be surveyed, exploited and protected. For NATO, this means that members must coordinate their design of cyberspace to be able to act collectively and support each other. This coordination simultaneously increases vulnerability. This will involve clearer standard operating procedures in the future, with the leading power, the United States, imposing its cyber culture as the benchmark. China does not have this challenge due to a lack of allies but will pass this on to interested governments via surveillance techniques.

For the two world powers, this defines a new space of capabilities that combines economic and military agency and produces conflicting cultures. The cooperative use of this space has failed so far, and the upcoming conflicts do not suggest a different development. A state with the ambitions of a world power cannot fall behind here. However, technological progress and production capabilities are not something that can be conquered militarily.

photo: private

Thomas Jäger, Chair of International Relations and Foreign Policy, University of Cologne, Editor of the Zeitschrift für Außen- und Sicherheitspolitik

documentation

ENISA Threat Landscape 2022

(Ed/nc) In November 2022, the European Union Agency for Cybersecurity (ENISA) published the tenth edition of its annual Threat Landscape report identifying major cyber threats, most affected sectors, and the impact of the Coronavirus pandemic and the war in Ukraine.

The eight top cyber threats

The ENISA report identifies eight major threat groups:

- **Ransomware:** hackers seize control of someone's data and demand a ransom to restore access
- **Malware:** software that harms a system
- **Social engineering threats:** exploiting human error to gain access to information or services
- **Threats against data:** targeting sources of data to get unauthorised access and disclosure
- **Threats against availability – Denial of Service:** attacks preventing users from accessing data or services
- **Threats against availability – Internet threats:** threats to the availability of the internet
- **Disinformation/misinformation:** the spread of misleading information
- **Supply-chain attacks:** targeting the relationship between organisations and suppliers

The six top sectors affected

1. Public administration/government (24% of incidents reported)
2. Digital service providers (13%)
3. General public (12%)
4. Services (12%)
5. Finance/banking (9%)
6. Health (7%)

The impact of the war in Ukraine

As regards the impact of Russia's war against Ukraine on cyberthreats, the report states that the cyber sphere has been influenced by the war in many ways. According to ENISA, cyber operations are used alongside traditional military action.

Hacktivist activity (hacking for politically or socially motivated purposes) has increased, with many conducting attacks to support their chosen side of the conflict.

Disinformation was used by both sides: Russian disinformation has focused on finding justifications for the invasion, Ukraine has used disinformation to motivate its troops.

Deepfakes with Russian and Ukrainian leaders expressing views supporting the other side of the conflict were also used.

Extorsion of money from people wanting to support Ukraine was tried by cybercriminals via fake charities.

Web ENISA report https://bit.ly/3RY547B

documentation

Protecting the cyberspace and societies

(ed/Céline Angelov, Linz) Cyberspace is the virtual space of all IT systems networked at the data level on a global scale. It is based on the internet as a universal and publicly accessible connection network, which can be supplemented and expanded by any other data network. The core business of critical sectors such as transport, energy, healthcare, and finance, but also democratic processes, space and defence is increasingly dependent on digital technologies. While digitalisation can bring enormous opportunities and solutions to many of the challenges Europe is facing, it exposes at the same time the economy and societies to growing cyber threats and crimes.

Cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; interrupting normal business processes, or influence people by disinformation. In the civil sector, massive attacks of disruption against governmental institutions, economy, industry, transport and energy networks, as well as information systems of open societies can paralyse a whole country. In the military sector, cyber-attacks will be able to paralyse all sorts of command and control and autonomous weapon systems. Implementing effective cybersecurity measures is particularly challenging.

EU Cybersecurity Strategy for the digital decade

On 16 December 2020, the European Union (EU) launched a new EU Cybersecurity Strategy covering the security of essential services such as hospitals, energy grids and railways. It also covers the security of the ever-increasing number of connected objects in people's homes, offices and factories. The objective of the Strategy is to develop collective capabilities to respond to major cyber-attacks and working with partners around the world to ensure international security and stability in cyberspace.

The Strategy contains concrete proposals for regulatory, investment and policy initiatives, in three areas of action:

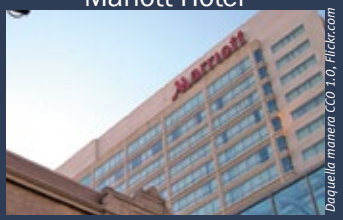
1. Resilience, technological sovereignty and leadership

The Strategy proposes to:

- reshape the rules on the security of network and information systems through a directive on measures to achieve a common high level of cybersecurity across the Union (Revised NIS Directive or "NIS2"),
- improve the resilience of critical public and private sectors: hospitals, energy grids, railways, but also data centres, public administrations, research laboratories and the manufac-

Major cyber-attacks 2014–2022

2014
Mariott Hotel

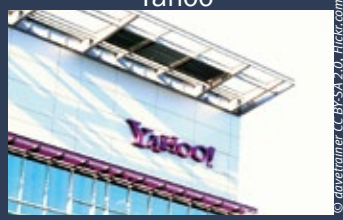


Daquella manera CCO 1.0, Flickr.com

WORLDWIDE

- The attack affected credit card details, passport numbers, and birthdates of 300 million guests stored in the brand's global guest reservation database worldwide
- Until 2018, the attackers continued to have access to all data, unrecognised
- The card numbers were encrypted using Advanced Encryption Standard encryption
- High officials fear the hack was instituted by a foreign nation looking to monitor travel plans of diplomats and government officials.

2016
Yahoo



© davetrainer CC BY-SA 2.0, Flickr.com

UNITED STATES

- Cybercriminals stole email addresses, passwords, telephone numbers, dates of birth and names from at least 500 million people
- The hacker was hired by Russian agents
- He was able to gain access to Yahoo's user database and account management tool through a phishing campaign which specifically targeted Yahoo's employees
- He installed a backdoor on a Yahoo server that allowed him to steal a copy of the user database and transferred it to his computer.

2016, 2017
Kyiv Airport Boryspil

©KEVIN HORGAN, CC BY 2.0, Flickr.com

UKRAINE

- Boryspil Airport in Ukraine experienced a wave of cyber-attacks on the country's critical infrastructure in 2016
- It was infected with the BlackEnergy malware and Russia is suspected to be behind it
- In 2017 there were more attacks that simultaneously affected multiple infrastructures and companies in countries such as Russia, Spain, Great Britain and France
- The GoldenEye ransomware caused the unavailability of parts of the IT equipment at Kyiv airport.

2021
Colonial Pipeline


© gawd, CC BY 2.0, Flickr.com

UNITED STATES

- Largest publicly disclosed cyber-attack against the Colonial Pipeline – one of the largest and most vital US oil pipelines and caused fuel shortages and panic buying
- Hackers identified the network through an exposed password for a VPN account and stole 100 GB of data within a two-hour window, infected the IT network with ransomware affecting computer systems, billing and accounting
- Colonial Pipeline paid the demanded ransom of $4.4m.

ture of critical medical devices and pharmaceuticals,
- build a network of security operations centres across the EU using artificial intelligence (AI), which will be a true 'cyber-security shield' for the EU, with the ability to detect early signals of impending cyber-attacks and enable action before damage is caused,
- support small and medium-sized enterprises (SMEs) within the framework of the "Digital Innovation Hubs" and increase efforts to educate and train specialists, especially in the area of cybersecurity.

2. Building operational capacity to prevent, deter and respond

The Strategy proposes to

- prepare a new common Cyber Hub to strengthen the cooperation between EU institutions and Member State authorities responsible for preventing, deterring and responding to cyber-attacks (including civil and diplomatic communities, as well as the cybersecurity law enforcement and defence communities),
- strengthen the EU Cyber Diplomacy Toolbox to prevent, deter and effectively respond to malicious cyber activities, in particular those affecting our critical infrastructure, supply chains and our democratic institutions and processes,
- improve cyber defence cooperation and develop cutting-edge capabilities in this field, relying on work of the European Defence Agency (EDA) and calling on Member States to use the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF).

3. Advancing a global and open cyberspace through increased cooperation

The Strategy proposes to

- intensify cooperation with international partners to strengthen the rules-based world order, promote international security and stability in cyberspace, and protect human rights and fundamental freedoms on the internet,
- promote international norms and standards that reflect the core values of the EU by working with its international partners in the United Nations and other relevant fora,
- strengthen their tools for cyber diplomacy,
- develop an EU agenda for building external cyber capacities in third countries,
- intensify cyber dialogues with third countries, regional and international organisations and the multi-stakeholder community,
- set up a global EU cyber diplomacy network to promote a common vision of cyberspace.

Web https://bit.ly/3Ik9Vgk

photo background: © africa-studio.com, stock.adobe.com

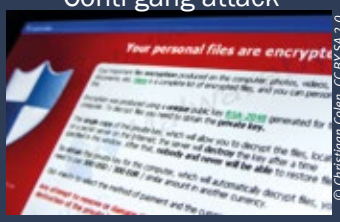
2021
JBS

© Visual Content, CC BY 2.0, Flickr.com

BRAZIL

- A ransomware attack by the REvil group against Brazilian meat-packing giant JBS disrupted production in the US, Canada and Australia
- JBS had to shut down all of its beef plants and some packaging centres
- The company was able to supply 25 percent less meat than usual, driving up the price of meat products
- JBS paid the hackers about $11m ransom in bitcoins.

2022
Conti-gang attack



© Christiaan Colen, CC BY-SA 2.0, Flickr.com

COSTA RICA

- A ransomware attack by the Russian-based Conti-gang against nearly 30 institutions of the government of Costa Rica, including its Ministry of Finance, the Ministry of Science, Innovation, Technology and Telecommunications, etc
- The adversaries gained access from the compromised VPN log by installing a crypted form of Cobalt Strike inside the Costa Rica sub-network
- Over 600 GB of data stolen from the attack have been leaked online.

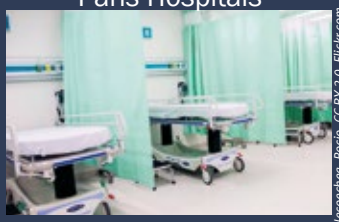
2022
Satellite modems

© Christiaan Colen CC BY 2.0, Flickr.com

UKRAINE

- A civilian/military cyber offensive by Russian hackers took place one hour before Russia's military invasion of Ukraine
- Thousands of Viasat KA-SAT satellite broadband modems were rendered inoperable in Ukraine, including those used by military and other governmental agencies
- The outage also disconnected modems used to control roughly 5,800 wind turbines in Germany and affected customers from Germany, France, Italy, Hungary, Greece, and Poland.

2022
Paris Hospitals



©Necpechtej_Rocio, CC BY 2.0, Flickr.com

FRANCE

- Hackers entered the IT systems of two hospitals near Paris and blocked access to their software for patient admissions
- No emergency patients could be admitted, operations had to be postponed and devices were out of order
- The hackers demanded a ransom of €10m to unlock the hospital software
- Since the hospital did not pay, the hackers published data on patients and staff on the dark web.

Documentation by Céline Angelov, member of the editorial team

Cybersecurity is a shared responsibility

The EU cybersecurity strategy for facing current and future threats

by Dr Roberto Viola, Director General,
DG CNECT, European Commission, Brussels

As the digital and the physical worlds are converging more and more, it is of utmost importance to enhance cybersecurity. Cyberattacks know no borders. Therefore, a comprehensive EU approach based on trust, solidarity and mutual assistance is key to fight current and future threats and to be a point of reference for other international actors.

European cyber resilience is vital

The war in Ukraine is only the tip of the iceberg of what we have been experiencing in the global security environment, which is becoming more contested, complex and interconnected. The cyber resilience of Europe and beyond is being challenged more than ever by both cyber – such as wipers, phishing, misinformation – and hybrid attacks.
Beyond the current conflict, as reported by the European Agency for Cybersecurity (ENISA), and in terms of the general cyber situation, local and public administration, government and healthcare form the most targeted groups in Europe. Incidents in the EU over the last year involve mostly ransomware cases by cybercriminal gangs, followed by hacktivist activity by Russian-led or otherwise pro-Russian threat actors. Hacktivists primarily attack institutions to have a greater media exposure, while criminals favour targets that are most likely to pay ransoms due to the relative high impact of the disruption (e.g. hospitals, service-providing public institutions). Cyber espionage also remains a growing threat.

> "Technology is constantly evolving, making our lives easier, bringing new opportunities, but also new risks. We are constantly learning, closely observing developments in the digital field, analysing potential difficulties and drawing possible scenarios."

Dr Roberto Viola

photo: European Commission

is the Director-General for Communications Networks, Content and Technology, (DG CNECT) at the European Commission since 2015. He holds a Doctorate in Electronic Engineering and a Master of Business Administration (MBA). Mr Viola served, amongst others, as Chairman of the European Radio Spectrum Policy group (RSPG) from 2012 to 2013 and Secretary General in charge of managing AGCOM from 2005 to 2012.

The EU has done its homework

In such a heightened threat environment, it is reassuring that the EU has done its homework to raise the resilience of our critical infrastructure. Almost 10 years ago, the Commission proposed the first EU-wide law on cybersecurity – the NIS Directive, which came into force in 2016. These rules laid the ground for improved EU level of cooperation and increased cyber resilience of the Member States.

Revised NIS Directive: The Directive has already been reviewed and will be soon repealed by the NIS2 Directive, which entered into force in January 2023. The NIS2 Directive will ensure an even safer and stronger Europe by significantly expanding the sectors and type of entities falling under its scope, streamlining incident reporting obligations, introducing more stringent supervisory measures and enforcement requirements for national authorities, and strengthening security requirements for companies.

Cybersecurity Strategy for the Digital Decade: Among the many initiatives to enhance cybersecurity the EU has provided since then is the EU's Cybersecurity Strategy for the Digital Decade, which focuses on building collective capabilities to respond to major cyber-attacks and working with partners around the world to ensure international security and stability in cyberspace. The Strategy announced €2bn in funding for cybersecurity under the EU research programmes, Horizon Europe, and the Digital Europe Programme. In addition to this, about €134.5bn of the €672.5bn Recovery and Resilience Facility consisting of grants and loans has been earmarked for investments in the whole digital technology supply chain.

Margaritis Schinas (left), Vice-President of the EU Commission, and Thierry Breton, Commissioner for the Internal Market, 15 September 2022

photo: European Union, 2022 – EC Audiovisual Service/ Aurore Martignoni

Cyber Resilience Act: The Strategy also mentions the need for the extension of cybersecurity obligations to the Internet of Things, which was addressed in a proposal for a new Cyber Resilience Act presented in September last year. The act will ensure that products with digital elements, such as wireless and wired products and software, are more secure for business users and consumers across the EU. The European Cyber Resilience Act will be another key milestone to raising Europe's cybersecurity across all domains and could set an example for our partners all over the world.

New EU Cyber Defence Policy: In November last year, the Commission and the High Representative put forward a new EU Cyber Defence Policy to address the deteriorating security environment following unjustified Russian aggression against Ukraine.
It sets the path towards stronger military and civilian cooperation on crisis management and information sharing. With both NATO and the EU calling for Member States to boost their cyber defence capabilities, it provides a strong framework for closer cooperation with NATO. The EU will have a key role to play through investing in research and development in areas such as Artificial Intelligence (AI) and quantum, which are crucial for cyber defence.
Last month, the third Joint Declaration on NATO-EU cooperation was signed, where the EU and NATO agreed to create a task-force on resilience and critical infrastructure protection, also addressing cybersecurity matters.
The Joint Communications on EU Cyber Defence Policy also announced that the Commission is preparing an EU Cyber Solidarity Initiative to strengthen common EU detection and situational awareness, and Member States preparedness and response capabilities to major cybersecurity incidents. It will do so by supporting the creation of a pan-European infrastructure of Security Operations Centres to improve cyber threat detection and analysis. It will also strengthen preparedness and response actions across the EU by gradually building an EU-level cyber reserve with services from trusted private providers and by supporting the testing of critical entities for potential vulnerabilities.

We will not stop here

The Union remains open to an ambitious and mutually beneficial cybersecurity engagement with all like-minded partners. For instance, we are cooperating closely with the United States, including through regular cyber dialogues, to enhance transatlantic cooperation to prevent, detect and respond to malicious cyber activities and protect critical infrastructure.
Moreover, the EU is continuously supporting Ukraine in building its cyber resilience. We will not stop here. Technology is constantly evolving, making our lives easier, bringing new opportunities, but also new risks. We are constantly learning, closely observing developments in the digital field, analysing potential difficulties and drawing possible scenarios. Cybersecurity is a shared responsibility and is more important than most think.

Web Further information

NIS2 Directive https://bit.ly/3HOLYvW
Cybersecurity Strategy https://bit.ly/3XmkZO5
Cyber Resilience Act https://bit.ly/3IIb72W
EU Cyber Defence Policy https://bit.ly/3YJQEdp

BDSV

Federation of German
Security & Defence Industries e.V.

SECURITY IS KEY TO SUSTAINABILITY

The member companies of the Federation of German Security & Defence Industries e.V. (**BDSV**) are highly qualified suppliers and partners of the German Armed Forces (Bundeswehr) and of the ministries entrusted with responsibilities regarding **national security**. Our industry is an indispensable part of German security interests and contributes to the **protection** and **security** of Germany's citizens.

We are convinced that there can be no sustainability without security.

CONTACT
Friedrichstrasse 60
10117 Berlin
+49 (0)30-2061 8999-00
bdsv@bdsv.eu
www.bdsv.eu

Disinformation, manipulation and interference

The new war of minds

by Jean-Dominique Giuliani, President of the Robert Schuman Foundation, Paris

On 7 February, the European External Action Service (EEAS) released its first report on foreign information manipulation and interferences (FIMI), which a 2015 European Council asked it to draft. The European Parliament has set up a Committee of Inquiry on the same subject, as have several national parliaments, most recently the French National Assembly. This report and this work shed light on the hostile actions of powers that have declared an information war on democracies. They shed light on hostile strategies and procedures that use every means possible to discredit our societies in which the first freedom is access to pluralist information in which citizens can freely form their opinions. Obviously, European society is one of the most liberal in this respect and therefore one of the most targeted by these activities. For the first time, by deciphering and analysing in a quasi-scientific way the messages peddled by these enemies, the EEAS gives a complete overview of the methods used, which can be summarised in 5 D's: Dismiss, Distort, Distract, Dismay and Divide.

Russia – a champion in disinformation

Denying and refuting with the crudest of lies, of which only dictatorships are capable; distorting and discrediting quality information; distracting attention with twisted procedures; threatening and frightening by spreading fear; sowing division everywhere, including between religions, ethnic groups and nations – these are, in short, the techniques used, which give priority to images, fake videos or the most vulgar editing. By saturating the digital space with these lies, their authors make the work of the press and journalists more difficult and allow "infiltrators", "fellow travellers" and their agents of influence to amplify their message and undermine the credibility of honest and objective information. Russia has been the champion of this since 2013-2014 and has increased its pressure since its aggression on Ukraine. One of the main interests of the EEAS work is to be able to attribute the spread of this disinformation to specific origins. The Russian troll factories are operating full out, and we now know where they come from, how they are financed and where they are located, but they find relays in the statements made by Russian diplomats and often by Chinese partners, official or unofficial. This proves that a power like Russia, still a member of the UN Security Council, is not afraid to spread false information about Ukrainian "Nazism", about the presence of American biological research laboratories in Ukraine, about the role of NATO or France in Africa. It seals its lies by relaying them through official allusions or actions by its Foreign Ministry and the Russian Presidency.

Europe's awakening

The European Union has belatedly become aware of this new hybrid war. Reluctant by nature to control information, our democracies can no longer ignore the action of what is far worse than a "fifth column", aimed at weakening support for resistance to the criminal actions of dictatorships. A Digital Media Observatory, initially based on a Code of Conduct, has been created by the European Commission, which has managed to attract the interest of the major global platforms. The Digital Services Act, adopted in 2022, which will come into force in 2024, gives the European Commission the power to oversee compliance with European rules, including abroad, which constitutes a form of extraterritoriality of European law. Finally, the work of the EEAS with its website EuvsDisinfo **(euvsdisinfo.eu)** represents a new stage in the European awakening. Disinformation is a real weapon that attacks the vulnerabilities of our free and open societies. Fighting its development is as much a necessity as the most basic civil and military defences that protect them. The multiple forms of "hybrid warfare", aggression emanating from nations or groups that do not have the traditional means of defeating our democracies, demand strong responses. They surprise us because freedom of thought, expression and association are part of the genes of democracy. But they also oblige us to defend these universal values whose enemies are now clearly visible. We must not weaken in this existential struggle.

> "Disinformation is a real weapon that attacks the vulnerabilities of our free and open societies."

Web: EEAS report: https://bit.ly/40Dvdg0

BLÜCHER®

PROTECTS

CBRN PERSONAL PROTECTIVE CLOTHING

PROTECTING THOSE WHO PROTECT US

www.bluecher.com

Protecting critical infrastructure

Lessons for Europe to learn from recent hybrid and cyber-attacks

by Prof Dr Angelika Niebler MEP, European Parliament, Brussels/Strasbourg

photo: Martin Lahousse

Do you remember the attacks in September 2022 on the Nord Stream gas pipelines that connect Germany and Russia? The four explosions that hit the pipelines were immediately suspected to have been carried out by Russia, as there were already major political tensions after the Russian invasion and ongoing war against Ukraine, as well as its consequences for the European Union (EU). Until today, there is no clear evidence on who attacked the gas infrastructure. The Nord Stream attack is not the only example of attacks on critical infrastructure in recent years. Another well-known incident happened in October 2022, when foreign hackers destroyed communication cables of the German railway Deutsche Bahn: public transport services were interrupted for several hours in northern Germany. Another particularly striking example is the ransomware attack on Irish hospitals in 2021 that paralysed hospitals for a whole week. Aggressors in cyberspace have increasingly been focussing on damaging critical infrastructure.

There are three lessons to be learned from cyber-attacks on critical infrastructure.

1. Cyber-attacks have become more dangerous.

For years, hybrid war has been an issue. However, the number of attacks on critical infrastructure is consistently increasing, thus exposing new vulnerabilities, as they can have a detrimental effect on society. In the digital age, our societal and economic ecosystems are closely connected to citizens: healthcare, transport networks, energy supply. Imagine if all the medical devices in a hospital could not be used anymore. No X-ray, no access to disease progression data, no medical analysis. During the ransomware attack in Ireland, doctors had to send their cancer patients home because they could not treat them. Without an adequate cybersecurity response, attackers can even disrupt supply chains that are of the utmost importance to the everyday life of citizens.

2. The EU plays an important role in coordinating national efforts towards protecting critical infrastructure.

In the European internal market, nearly all grids and networks are connected, be it in energy, telecommunications, transport or aviation. For that reason, there is a risk that the disruption of infrastructure in one Member State can affect the

Prof Dr Angelika Niebler

has been a Member of the European Parliament (EP) since 1999. She chairs the CSU Group in the EP and is co-chair of the CDU/CSU Group. Holding a doctorate in law, she is a member of the Committee on Industry, Research and Energy, (ITRE), a substitute member of the Legal Affairs Committee (JURI) and of the Special Committee on the COVID-19 pandemic: lessons learned and recommendations for the future (COVI). She is also a member of the EP's Delegation to the US. Angelika Niebler has been deputy party chair of the CSU since 2015 and was elected president of the Union Economic Advisory Council in 2018. Since 1991, she has worked for various law firms in Munich. Besides her work as a lawyer, she is a professor for Business Administration/Applied Business Innovation at the University of Applied Sciences in Munich.

→ *Continued on page 28*

> "The EU plays an important role in coordinating the Member States' efforts towards more cybersecurity."

whole European-wide network. Thus, we need high cybersecurity standards throughout the EU to protect our connected infrastructures. The EU plays an important role in coordinating the Member States' efforts towards more cybersecurity. For instance, the **European Union Agency for Cybersecurity** (ENISA) engages in sharing the Member States' knowledge, building capacity and raising awareness in the field of cybersecurity. Coordination is important so that Member States can learn from each other and be alerted swiftly in case of an emergency.

3. Adapting to emerging threats is key.

Adapting to the threats that are emerging with hybrid and cybersecurity attacks on critical infrastructure is key. The EU is in fact already doing so. In 2016, the **Directive on security of Network and Information Systems** (NIS1 Directive) entered into force, which obliged Member States to build up national capacities for cybersecurity. According to this directive, any attack on critical infrastructure has to be notified to the competent authority immediately. With the **Directive on measures for a high common level of cybersecurity across the Union** (NIS2 Directive), the EU modernised these cybersecurity measures for critical infrastructures. The new legislation entered into force in January 2023. What is new: new sectors and entities, such as cloud computing service providers, data centre service providers and operators of ground space infrastructure, are now also within the scope of the existing cybersecurity rules. Further, every Member State is required to set up a "Computer Security Incident Response Team" to respond in emergency cases. A new "Cooperation Group" will facilitate the exchange of information between the EU Member States. The NIS2 Directive also introduces more detailed reporting obligations for cyber-attacks. Attacked companies are obliged to send an early warning. This update of the EU cybersecurity measures was the right step towards protecting our critical infrastructure.
Further to the NIS2 Directive, the EU is also making efforts to better protect the infrastructure of its own public institutions. To this end, in March 2022, the EU Commission proposed a **Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union**, which is currently under consultation in Council and Parliament.
However, despite all efforts to counter cyber-attacks, it should always be clear that you cannot prevent them, you can only minimise the risk and arrange for immediate response.

documentation

Illustration: ESDU/KonawatTH, stock.adobe.com

(Ed/nc, Paris) The 2016 Network and Information Security (NIS) Directive was the first piece of a EU-wide legislation aimed at increasing Member States' cybersecurity capabilities. To respond to the growing threats posed with digitalisation, the existing legal framework was updated by the **Directive on measures for a high common level of cybersecurity across the Union** (NIS2 Directive) that came into force on 16 January 2023. The scope of the cybersecurity rules was expanded to new sectors and entities that are obliged to take security measures. The aim is to further improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

The NIS2 Directive will:
Strengthen Member States' preparedness, by requiring them to be appropriately equipped, e.g., with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.
Foster the cooperation among all the Member States by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
Build a culture of security across sectors that are vital for the economy and society, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.
web **https://bit.ly/3Ifrmxf**

Security and Defence

German Federal Chancellor Olaf Scholz at the Berlin Security Conference, 30 November 2022

photo: @Boris Trenkel

European Parliament

2022 Annual Report on the CSDP

On 18 January, the European Parliament adopted in a plenary session the 2022 Annual Report on the Common Security and Defence Policy (CSDP). The report, drafted by MEP **Tom Vandenkendelaere** (EPP, Belgium) for the Foreign Affairs Committee (AFET), focuses in part on Russia's aggression against Ukraine and the EU's response, the implementation of the Strategic Compass, the EU defence initiatives and the parliamentary scrutiny of the CSDP.

Ukraine: MEPs stress the dramatic deterioration of the security situation in Europe resulting from Russia's aggression against Ukraine. They call on the European Union (EU) to step up and accelerate its efforts to provide Ukraine with the necessary financial, humanitarian and military aid and equipment, including heavy weaponry.

EU initiatives: The report welcomes the new EU initiatives aimed at enhancing cooperation on security and defence such as the Versailles declaration, the Strategic Compass, the defence investment gap analysis, and the proposal on EDIRPA (European Defence Industry Reinforcement through common Procurement Act). As regards the Strategic Compass, the report considers it a "major impetus that could generate the necessary momentum towards a genuine European Defence Union". It calls for the Rapid Deployment Capacity, a modular force of up to 5,000 personnel, to be implemented "as soon as possible and by 2025 at the latest".

CSDP missions: The report underlines that CSDP missions and operations need to be more closely aligned with the needs of the host countries, and calls for more "robust and flexible mandates" for them, as well as adequate resources, staffing, funding, training and equipment.

Parliamentary scrutiny: Finally, the report calls for increased parliamentary scrutiny of the CSDP and the creation of a fully fledged Council formation for defence.

"Last year was an extraordinary year in terms of Security and Defence Policy. (...) A year of realising that we must do much more for our security."

Rapporteur Tom Vandenkendelaere MEP during the plenary debate on 18 January 2023

photo: ©European Union, 2023 – source: EP

Web https://bit.ly/3HUGUWX
Video https://bit.ly/3YK0A6H

Swedish Presidency

Reinforcing EU defence partnerships

A more secure Europe, with the EU as a stronger security and defence actor is one of the Swedish EU Presidency priorities. The Presidency conference on **"Reinforcing EU Defence Partnerships"**, held from 30 to 31 January at Uppsala Castle in Sweden, focused on the **EU's cooperation with strategic partners.** The event gathered some hundred participants, among them EU defence policy directors, representatives from various EU institutions as well as a number of the EU's strategic partners such as representatives from the United States, the United Kingdom, NATO, Norway, Canada and Iceland. A report on regional defence cooperation and EU cooperation with strategic partners was presented by the European Union Institute for Security Studies (EUISS).

In his opening speech, **Swedish Minister for Defence Pål Jonson** underlined the responsibility of the EU Presidency in the times of the ongoing Ukraine war. He said: *"A heavy responsibility rests on the Swedish Presidency at this crucial time in our Union's history. That is why the priorities of the Swedish Presidency focus on meeting the challenges we face in this difficult security situation. Sweden has three main priorities in the area of security and defence: support to Ukraine, the implementation of the EU's Strategic Compass and strategic partnerships."*

Swedish Minister for Defence Pål Jonson speaking at the conference held at the Uppsala Castle, Sweden

photo: ©Axel Öberg/Government Office of Sweden, CC BY-ND 2.0, Flickr.com

At a number of panel discussions focussed on **regional and multilateral cooperation,** representatives from the European Intervention Initiative (EI2), the Joint Expeditionary Force (JEF) and the Nordic Defence Cooperation (NORDEFCO) gave their perspectives. Another panel discussion focused on the question of how **cooperation between bilateral strategic partners and the EU** can be developed.

The conference's final panel discussion was dedicated to the **role of the Union and NATO in European security,** in light of the Joint Declaration on EU-NATO cooperation signed on 10 January. The panel participants discussed how the implementation of the EU's Strategic Compass and NATO's new strategic concept can generate more new areas of cooperation.

From left to right: European Council President Charles Michel, NATO Secretary General Jens Stoltenberg and European Commission President Ursula von der Leyen after the signature of the Joint EU-NATO Declaration, Brussels, 10 January 2023 photo: NATO

A more capable and therefore autonomous EU would strengthen the transatlantic bond

NATO's European pillar – what does it mean for European security and defence?

Interview with Michael Gahler MEP, European Parliament, Brussels/Strasbourg

The European: *Mr Gahler, you have been dealing with security and defence issues in the European Parliament since 2004 and have held leading positions both in your party and in Parliament. As a member of the Foreign Affairs Committee (AFET) and a substitute member of the Subcommittee on Security and Defence (SEDE), you are strongly involved in European defence issues. What does it mean for you that the European Union engages its defence capabilities as a pillar in NATO?*
Michael Gahler: Soon the number of EU Member States in NATO will amount to 23, thereby further increasing the EU's weight in NATO. However, the capabilities of these 23 are still far behind those of the United States (US). Strengthening the European pillar within NATO means first and foremost that EU countries fulfil their commitments towards NATO as expressed in the 2% goal. Living up to that ambition would strengthen the European contribution to transatlantic security, provided, of course, that this money is also better coordinated and jointly invested in the development and procurement of armaments and technologies.

The European: *To that end, can the EU function as a facilitator?*
Michael Gahler: Indeed, the EU can be a facilitator through the European Defence Fund (EDF) and the future European Defence Investment Programme (EDIP) which provides additional money for defence. And money is something that NATO cannot provide. Nonetheless, it is vital to ensure coherence and close cooperation between the EU and NATO when it comes to defence planning and capability development. Unfortunately, the recent third EU-NATO Joint Declaration of 10 January did not indicate that there will be a new and deeper dynamic in coordinating EU-NATO cooperation.

The European: *Does that mean, Mr Gahler, that we should not refrain from political demands in discussion that there should be "European autonomy" in matters of defence?*
Michael Gahler: There is no doubt that NATO is and remains the backbone of our collective defence in Europe. However, given that about 80% of the so-called strategic enablers within NATO are provided by the United States and considering that US capabilities might in future become increasingly bound in the Indo-Pacific, EU-NATO members should improve their capabilities in that area.
That is also vital in cases where NATO does not want to engage in a given scenario, or where access to the Alliance's capabilities for an EU operation is blocked by certain NATO members.

→ *Continued on page 32*

The European: *In such cases, the EU should be able to act on its own.*
Michael Gahler: A more capable and therefore autonomous EU would indeed strengthen the transatlantic bond as we Europeans would have more to offer our transatlantic partners and could ease the burden on the US. For me, a strong European defence technological industrial base is also an integral part of "strategic autonomy".

The European: *Does that not also lead to unnecessary duplications? Why do we need a European Rapid Deployment Capacity (RDC) if we have the NATO Response Force (NRF)?*
Michael Gahler: I do not consider the EU's RDC a duplication of NATO's NRF, especially under recent circumstances. Until Russia's war of aggression the NRF was mostly deployed in disaster relief operations. With NATO's new force posture following 22 February 2022, the NRF became a core element to deter Russia and if necessary, defend Europe. Therefore, for the time being it is highly unlikely the Alliance would deploy these troops for crisis management operations. While Russia's war is indeed the biggest security threat we are currently facing, other crisis areas tend to be overlooked, notably in Africa. There, the EU is engaged in different missions and operations in a volatile security environment. In overseen developments, we need to react quickly, at least to evacuate our citizens and personnel.

The European: *So, the primary task for the RDC would be crisis management?*
Michael Gahler: Yes, however, I also foresee an option to temporarily assign the RDC to NATO in case of need, thereby achieving conjunction rather than duplication between the two organisations if we ensure the RDC's compatibility with NATO standards.

The European: *Your answer brings me to the issue of work sharing, which means that not every country should procure everything, but systems must be interoperable and complement each other. Is this the future for European defence procurement?*
Michael Gahler: Ideally yes. EU Member States already committed to a level of joint defence investment of 35%. In 2021 we only reached 18%, a huge gap to fill. To finally move closer to a capable European Defence Union, coordinated joint investments are vital as only a joint approach can ensure interoperability and complementarity of systems as well as adequate economies of scale, saving European taxpayers' money. With the so-called EDIRPA regulation that aims to refill defence stocks that have been depleted because of the support given to Ukraine, we are already making an important step in that regard. But the decisive step will be the subsequent larger and long-term orientated European Defence Investment Programme (EDIP). Its ambition should be to close the gap between the Member States' commitment to joint defence investment achieved thus far. Translated into numbers, that would require a budget of at least €10bn for the period 2024 to 2027.

> "We recognise the value of a stronger and more capable European defence that contributes positively to global and transatlantic security and is complementary to, and interoperable with NATO."
>
> EU-NATO Joint Declaration, 10 January 2023

The European: *The European Defence Technology and Industry base (EDTIB) has as objective to foster European armament industries. It seems that there is still more splitting than cohesion. What are the reasons?*
Michael Gahler: I see two main reasons for that. Firstly, the fragmentation of the European defence market is a consequence of the fragmented demand in procurement in close conjunction with national industrial considerations by EU Member States. EU Member States prefer to award procurement calls to their national champions, neglecting the European perspective. The European Defence Fund already provided some remedy by bringing national industries closer together. However, breaking that structure and moving towards a real European Defence Technology and Industrial Base (EDTIB) will require EU Member States to also move towards joint procurement. As mentioned before, EDIRPA and EDIP can provide a big step forward to that end.

The European: *Does Europe need armament cooperation with the United States?*
Michael Gahler: Of course. The US are not only Europe's most important partner, but they also possess a very developed and capable defence industry providing sophisticated and fully developed military equipment covering the full capability spectrum that can be bought off the shelf. In light of Russia's war of aggression against Ukraine, the latter is crucial to improve European defensive capabilities that are urgently needed.

The European: *Mr Gahler, I am grateful for this conversation.*

The interview was led by Hartmut Bühl on 7 February 2023.

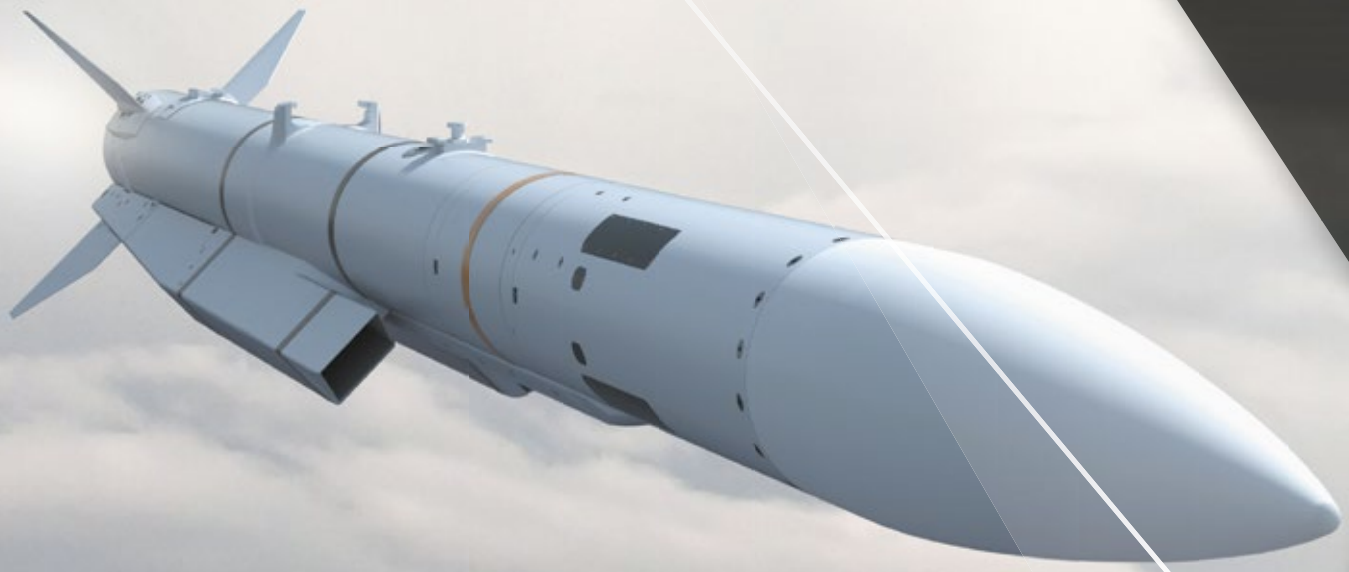
Web: Joint EU-NATO declaration https://bit.ly/3xgjvKM

Michael Gahler MEP

has been a Member of the European Parliament since April 1999. He is currently a member and the coordinator of the Foreign Affairs Committee (AFET), a substitute member of the Security and Defence Subcommittee (SEDE) and a substitute member of the Transport and Tourism Committee (TRAN).

MBDA
MISSILE SYSTEMS

EXCELLENCE AT YOUR SIDE



OUR COMMITMENT TO YOU

Armed forces face increasingly complex engagement scenarios where there is no room for error. In this demanding environment you can count on our expert teams who are committed to bringing you cutting edge, combat-proven technology and autonomy in defence.

SECURING THE SKIES

PROTECTING YOUR ASSETS

MASTERING THE SEAS

COMMANDING THE COMBAT ZONE

mbda-systems.com

Cooperation is part of the European Defence Agency's "DNA"

Requirements for forces in times of a challenging security environment

Interview with Stefano Cont, Director Capacity, Armament & Planning (CAP), European Defence Agency, Brussels

The European: *Director, when you took over your position in April 2022 you declared: "At a time when defence expenditure is expected to increase significantly (…), European cooperation and collaborative capability development will be key to making sure the money is spent well and efficiently." After a year of war in Ukraine, we are seeing closer cooperation between NATO Member States, but we are also observing some European nations going it alone in procurement. Can you describe the European Defence Agency's (EDA) central role in making cooperation and coordination possible?*
Stefano Cont: Cooperation is part of our DNA at EDA. Our mission is to enable cooperation between our members. What we have witnessed with the change in the environment is a greater willingness to cooperate within the European Union (EU) and particularly within the structures of the EDA. So much so in fact that the Steering Board is currently considering the establishment of three additional projects to meet the needs of many participating Member States (MS) in joint procurement.

The European: *What factors explain this achievement?*
Stefano Cont: This has only been achieved because EDA is a lean and agile organisation that can react speedily to Member States' demands and we are prepared to meet those needs in whatever way they suggest. This points to the relevance of the Agency in that it can respond to crises while still undertaking its core functions and without losing focus on immediate demands and issues.

The European: *Within these wide-ranging requirements, what is your strategy as EDA's Capability, Armament and Planning Director?*
Stefano Cont: Part of my remit is not just to develop capabilities but also to engage in armaments procurement. This is all the more necessary in view of the changing economic environment within which we have to work. With the increases in defence spending, there is a necessity to ensure that needs are balanced and that no one MS who wishes to have our assistance is left behind. Therefore, the methods of coordination which we employ on behalf of the MS are critical to the success of their endeavours. If the MS are successful, the EDA has served its purpose.
Overall, we need to ensure that the level of cooperation to meet short-term needs is expanded and enhanced to take in the medium-and long-term perspectives, thus ensuring that Europe has what it needs, on the basis of a common view of what the defence landscape should look like in the future.

The European: *Director, only 18% of all investments in defence programmes are conducted in cooperation. It seems that MS only seek cooperation when they have no national industrial capabilities or when the partner accepts the given military requirements. What are the consequences of this attitude for the MS's Capability Development Plan (CDP)? How much power do you have to influence MS?*
Stefano Cont: What you must remember is that the CDP gives rise to the EU Capability Development Priorities that are agreed by the Ministers of Defence for all EDA participating MS. These are not simply EDA priorities, and they are not developed in isolation. They are developed with the active participation and involvement of all our MS to ensure that we have an overall picture of where our priorities should lie.

> "EDA is a lean and agile organisation that can react speedily to Member States' demands."

Stefano Cont

photo: EDA

has been Capability, Armament and Planning Director at the European Defence Agency since 1 April 2022. Born in Trento in 1963, he received a doctorate in International and Diplomatic Sciences from the University of Trieste. He served in the Italian Air Force as a command pilot. Prior to his current assignment he worked as Defence Attaché in Washington D.C. for the US, Mexico and Canada after having served for many years as Head of the Political Military Office in the Cabinet of the Minister of Defence in Rome.

EDA Fire Blade helicopter exercise in Hungary, 21 June 2022

photo: © European Union, 2022/Peter Kohalmi

The European: *And what level of cooperation in defence programmes is required?*
Stefano Cont: There must be an alignment of several factors in order to raise the level of investment that is undertaken cooperatively. The difficulties that we have encountered in the past few years have been different planning horizons in MS and budgetary frameworks and laws that are different in all our MS, as well as the different needs and aspirations for national defence.

The European: *How important are geographical factors?*
Stefano Cont: We realise that the geographical position of one MS can entail totally different requirements to that of another, located in another area. Notwithstanding this, we continue to promote joint investment to the greatest extent possible. Again, this comes back to my remit within the armament procurement regime. We have shown that we can obtain speedy and positive results. And we mustn't forget that investment in a country's defence is not just in defence programmes as such, but across the whole range of activities that the militaries and defence forces of our MS must undertake.

The European: *And what influence can the EDA exert there?*
Stefano Cont: This is an area that covers doctrine, training, material and personnel and not just high-end armament programmes. To ensure success, we must help our MS focus on all areas of their activity and develop joint planning and a joint view of the future of European defence, encompassing planning, armament and capability development.

The European: *You are at the interface of the Permanent Structured Cooperation (PESCO) and the Coordinated Annual Review on Defence (CARD). Could you briefly describe how CARD and PESCO are linked?*
Stefano Cont: There is a symbiotic relationship between CARD and PESCO, as well as with the other European defence initiatives. CARD should be seen as the pathfinder for PESCO. CARD tells us where we stand and where we should be going, collaboratively. PESCO is one of the vehicles through which we can collaborate in developing our capabilities. However, PESCO is not just about capabilities. The more binding commitments for each Member State associated with this initiative are even more important. The clue is in the title – PERMANENT and STRUCTURED COOPERATION. The Member States, who are the driving-force behind PESCO, have been striving to attain this goal since its establishment. CARD enables us to review how the MS are developing to ensure that there is a structure and a permanence to the cooperation they undertake.

The European: It seems that there is a long road ahead..
Stefano Cont: ...yes indeed! What CDP, CARD and PESCO allow us to do is to align our planning processes, which is the basis on which a secure Europe can be built. This allows us all to travel in the same direction, if not necessarily at the same speed. As I indicated earlier, the needs of one MS will be different to that of the next, but with a knowledge of our MS' future planning, we can assist them in attaining their goals, which will then benefit all of Europe.

The European: *Let us finally have a look at an issue that gained importance, in particular since the start of the war in Ukraine: the mitigation of Chemical, Biological, Radiological and Nuclear (CBRN) threats. What is EDA's approach in these fields?*
Stefano Cont: EDA and specifically my directorate, have been extremely active in the whole area of CBRN for the last 10 years and not just since the start of the war in Ukraine. For the past three years, EDA has been running a specific project regarding CBRN to develop a joint approach to CBRN needs and requirements, particularly in the field of sensors. Furthermore, CBRN is one of the areas that we are currently preparing for MS joint procurement. This area will become even more important in the future and EDA will be at the forefront to ensure that our defence personnel receives the best equipment possible.

The European: *Director, I thank you for this conversation.*

The interview was led by Hartmut Bühl.

STOOF®
INTERNATIONAL

TROJAN® mit Höchstschutz

+++ Der LC 300 TROJAN VR9 mit Bestnoten +++

Zertifizierung nach VPAM ERV und BRV Fassung 3 mit drei von drei Sternen
Höchstschutz Seitenansprengung auf 2 Meter Abstand !

Zertifizierung nach STANAG 4569 AEP-55 Volume 2, Level 2a

STOOF International GmbH
Wurzelweg 4 · 14822 Borkheide · Germany
Tel: +49 (0)33845. 90-300 Mail: info@stoof-international.de
www.stoof-international.de

The Berlin Security Conference 2022

Conference report by
Hartmut Bühl, Publisher, Paris

photos: © Boris Trenkel

> **"Russia must not be successful in its actions under any circumstances. Autocracies must never prevail over democracy."**
>
> *NATO Secretary General Jens Stoltenberg speaking at the BSC in Berlin*

The 21st Berlin Security Conference (BSC), which took place from 30-31 November 2022 had a very special character. Never before has a BSC been held in wartime in Europe; never before have there been so many high-ranking speakers from the European Union (EU) and NATO countries, and never before has a BSC been so gender-balanced. This was only possible because this conference has been systematically built up over more than twenty years. Two decades of stimulating discussions geared towards shaping European security within the transatlantic security area, including its geostrategic aspects, have made the conference the most important Europe-wide discussion forum for the European security community.

The geostrategic interest of great powers...

While the basic conditions for European security and their implementation have so far focused more or less on Europe alone, this latest conference made a leap into broader geopolitical issues and shed light on the geostrategic interests of great powers and their consequences for European security. This year's conference partner, Norway, with its unique geopolitical experience, played a significant role in exploring the topics in more detail. High-ranking representatives from politics, business and civil society from Europe, the United States (US) and Asia gave an insight into their assessment of the security situation after the Russian invasion of Ukraine and sketched out the political and social consequences of this turning point for European societies.

...and focus on the war in Ukraine

All speakers agreed that EU and NATO support is paramount to Ukraine's survival but that the EU and NATO should not be dragged into the war. The conference requested European leaders to reinforce European capabilities to allow the EU as a pillar of NATO to gain the ability to defend its territory. This includes, besides strong land forces, air superiority and maritime capabilities, but also the strategic use of space and the mastery of cyberspace, which, in the context of international tensions, low-intensity conflicts and hybrid warfare, has gained prominence. Conference participants agreed that Germany now hosts the two most important and complementary conferences on security issues: the Munich Security Conference (MSC) and the independant Berlin Security Conference (BSC).

Speakers at the BSC

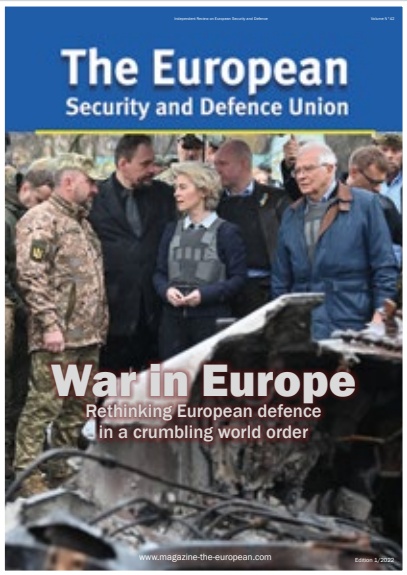
Keynote speakers from politics, military and industry included, amongst others:

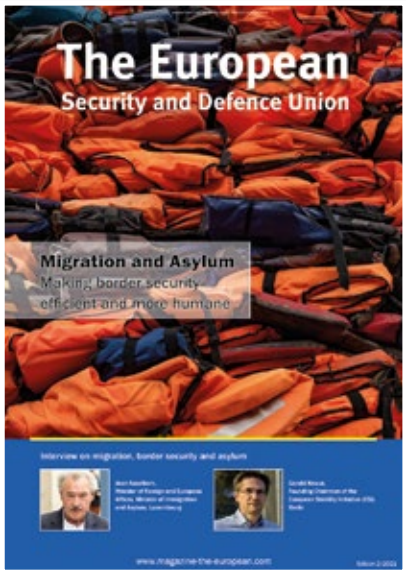
Olaf Scholz, Federal Chancellor of Germany,| **Jonas Gahr Støre,** Prime Minister of Norway | **Jens Stoltenberg,** NATO Secretary General | **Christine Lambrecht,** Federal Minister of Defence, Germany | **Bjørn Arild Gram,** Minister of Defence, Norway | **Antti Kaikkonen,** Minister of Defence, Finland | **Dr Pål Jonson,** Minister of Defence, Sweden | **Kristóf Szalay-Bobrovniczky,** Minister of Defence, Hungary | **General Christian Badia,** Deputy Supreme Allied Commander Transformation, Norfolk, NATO | **General Robert Brieger,** Chairman EU Military Committee | **Hans Christoph Atzpodien,** General Manager BDSV | **Micael Johansson,** CEO Saab, | **Udo Littke,** CEO ATOS...

Web: **https://www.euro-defence.eu/**

Our Authors in 2022

The leading magazine for Europe's security and defence community





The magazine is the first winner of the CIDAN European Award for "Citizenship, Security and Defence", organised in 2011 under the patronage of Mr Herman Van Rompuy, President of the European Council, in order to reward outstanding efforts towards promoting European citizenship and European security and defence awareness.
On 26 November 2019, the magazine was awarded from the same organisation with the CIDAN Special Jury Prize for its outstanding quality and efforts in promoting European citizenship, security and defence.

MEDIA AND CONTENT SALES / SUBSCRIPTION FOR DIGITAL AND HARD COPIES
Hartmut Bühl • Publisher and Editor-in-Chief
Phone: +49(0)172 32 82 319 E-Mail: hartmut.buehl@orange.fr

For further information: www.magazine-the-european.com


"I need reliable connectivity to be able to protect you.
Bittium Tough Mobile 2 Tactical
Meet Bittium experts at AFCEA Bonn, stand F14.
40 years of Finnish technology
www.bittium.com
Bittium