【欧州】【Common】

Common – IoT and transport infrastructure security: The problem of securing the EU's critical infrastructure in the light sabotage acts against the gas pipelines in the Baltic Sea

Andrea Antolini　Former Researcher JTTRI

【概要：Summary】

The destruction of most of the gas pipelines Nord Stream I and Nord Stream II in the Baltic Sea, which was apparently caused by an act of sabotage, has underlined the increased threat of potential hybrid attacks against Critical infrastructures (CI) of national and European importance, including transport infrastructures. Also, the act of sabotage against the Deutsche Bahn that caused the standstill of trains in the northern part of Germany, shows that such attacks can target any critical infrastructure in the EU, including transport systems.

In recent years, several concepts of protection of CI against physical and cyber threats or hybrid warfare have been discussed, and legislation has been introduced also at EU level to improve the protection, resilience, and the cybersecurity of CI, including transport infrastructure. In 2006, the Commission launched an EU programme for critical infrastructure protection (COM (2006) 786 final, and regarding hybrid attacks, the European Commission published a Joint Framework on countering hybrid threats (JOIN/2016/018 final). In December 2020, several proposals were presented to improve the protection of CI against cyberattacks or hybrid attacks and the resilience of CI. The proposal for a Directive on the resilience of critical entities (the "CER Directive") (COM (2020) 829 final) addresses the need to reduce the vulnerabilities of the critical entities which are essential for the functioning of the economy and replaces the current Directive 2008/114/EC on European critical infrastructure.

On 25 May 2022, the Commission presented the Fourth Progress Report on the implementation of the EU Security Union Strategy, and if the EU can adapt to exceptional and unexpected threats (COM (2022) 252 final. On 28 June 2022, the European Council and the European Parliament reached political agreement on the new CER Directive. The new rules cover eleven sectors of critical infrastructures including energy and transport, to strengthen their resilience against a range of threats.

Regarding the strengthening of the preparedness and resilience of the EU's transport sector in particular, the Commission presented a new Contingency plan for transport (COM/2022/211 final), which draws lessons from both the COVID-19 pandemic and Russia's military aggression against Ukraine. It proposes a toolbox of 10 actions to guide the EU and its Member States when introducing emergency crisis-response measures and highlights the importance

of regular resilience testing for different crisis scenarios.

However, the question is what measures the EU Member States could take to better protect CI and at best prevent such hybrid attacks. As the recent incidents and attacks confirm, the EU's CI is vulnerable against hybrid attacks and the currently elevated level of hybrid warfare during the ongoing Russian war in Ukraine. While the vast array of CI targets in the EU might never be fully defensible, there is no doubt that the EU's CI needs to be better protected against an increasing number of cyber threats, hybrid attacks or sabotage.

【記事：Article】

1. Sabotage cases: The destruction of NS 1 and NS 2 gas pipelines and sabotage against Deutsche Bahn

On 26 September 2022, the gas pipelines Nord Stream 1 (NS 1) and Nord Stream 2 (NS 2) in the Baltic Sea, which were mainly constructed to transport gas from Russia to Germany were damaged by explosions. The incidents were apparently caused by deliberate action of sabotage against the pipelines, according to the Council of the EU (2022a). Whereas the NS 2 had not been certified to transport gas, yet, and the process had been terminated due to the outbreak of Russian war in Ukraine, the NS 1 pipeline had been used to transport gas since years until recently, when the Russian company Gazprom reduced and eventually interrupted the transport of gas.

The explosions caused three leaks were detected on 26 September 2022 and a fourth leak had been confirmed on 29 September 2022. After months of deliberate reductions of gas exports by the Russian majority state-owned energy corporation Gazprom, the partial destruction of the pipelines has only left one pipe of non-certified NS 2 to be used for gas transport.

Following the meeting of the Swedish Government's security policy council on 28 September 2022, Prime Minister Magdalena Andersson and Minister for Foreign Affairs Ann Linde commented that the explosions were a deliberate act of sabotage, and that the leaks were located in the Swedish and Danish economic zones (Government offices of Sweden 2022). The EU emphasised to take further steps to increase the EU 's resilience in energy security (Council of the EU 2022a).

Furthermore, on 8 October 2022, Deutsche Bahn experienced a "sabotage acts on the cable network", which interrupted radio contact and data transmission between trains and the railway operating centres. This caused a serious interruption of train service of long-distance, regional and cargo trains in large parts of northern Germany, mainly the north-western states of Hamburg, Schleswig-Holstein, Lower Saxony, and Bremen for about three hours.

While authorities are investigating in both cases and the perpetrators are still unknown, these acts of sabotage underline that a period of incidents of hybrid warfare might only be starting. The question that arises is if the EU and its Member States are ready to secure their critical infrastructure and if enough measures are taken at EU level to have a common approach to improve the security of the EU's CI.

2. Hybrid warfare against CI

The recent incidents in Europe underline that the time of peace is changing towards a time of hybrid warfare in the wake of Russian war in Ukraine.

Hybrid warfare blurs the usual borders of peace and war, legal and illegal. According to the commander of the new Territorial Command of the German Bundeswehr, Lieutenant General Carsten Breuer, hybrid warfare is a combination of classic military operations, economic pressure, hacking attacks on infrastructure and even propaganda in media and social networks and related incidents that opposing powers use to create instability (Hoffmann 2022). Kalniete and

Pildegovičs (2021) use the term “hybrid threats’ a coverage for a range of destabilising and synchronised civil and military actions. Hybrid attacks can constitute a broad array of activities, such as cyber-attacks, election interference and attacks on critical infrastructure. It is coordinated and synchronized with the target to increase a state‘s and institution‘s vulnerabilities (Hybrid CoE n.d.). In its Joint Framework JOIN/2016/018 final), the European Commission defines hybrid threats as a “…mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare“ (European Commission 2016).

Hybrid attacks turn the vulnerabilities of the target into a direct strength for the hybrid actor, aiming to influence a state’s decision-making at the local, regional, state level and to undermine public trust in government institutions or exploiting social vulnerabilities (European Commission 2016, Hybrid CoE n.d.).

By using unconventional and conventional means, hybrid attacks cannot easily be attributed to certain actors, and this complicates to prevent or respond to them. In fact, regarding the gas pipelines NS 1 and NS 2, and Deutsche Bahn, it is still unclear who is responsible for the attacks, but both acts of sabotage have taken place during the Russian war in Ukraine. Regarding the act of sabotage against the NS 1 and NS 2 pipelines, it involves a high level of technical knowhow, which could only be provided by a state or a non-state actor with potential warfare experience. Known as “seabed warfare”, there are several countries that have the potential, operational assets and specialized forces for planning and executing such a hybrid attack (Hybrid CoE n.d.).

3. Legislation on securing and enhancing resilience against hybrid threats

In 2006, the European Commission started to introduce programmes and legislation to protect its CI against cyber and hybrid threat. The Communication (2006) 786 final sets out the principles, processes and instruments proposed to implement European Programme for Critical Infrastructure Protection (EPCIP) to improve the prevention, preparedness, response, and protection of CI in the EU (COM(2006) 786 final). The EPCIP framework consists of procedures for the identification and designation of European Critical Infrastructures (ECI), measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), and the support for Member States concerning National Critical Infrastructures (NCI) among others (COM(2006) 786 final).

Furthermore, the EU adopted the European Critical Infrastructure (ECI) Directive in 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (ECI Directive) (Council Directive 2008/114/EC).

The ECI Directive (2008/114/EC) of 8 December 2008 applies only to the energy and transport sectors and provides a procedure for identifying and designating ECIs, the disruption or destruction of which would have significant cross-border impacts in at least two Member States (Council Directive 2008/114/EC). It also sets out specific protection requirements on ECI operators and competent Member State authorities. 94 ECIs had been designated, of which two-thirds are located in Member States in Central and Eastern Europe. However, the scope of EU action on CI resilience extends beyond these measures and includes sectoral and cross-sectoral measures including climate proofing, civil protection, foreign direct investment, and cybersecurity. Meanwhile, EU Member States themselves have also

taken measures of their own action in this area but, due to the generality of some provisions and the different interpretations in EU Member States, the Directive 2008/114/EC only partially achieved its objectives.

In view of recent technological, economic, social, policy/political, and environmental developments and considering the new and evolving challenges in protecting Critical Infrastructure, the ECI Directive was evaluated in 2019.

The evaluation found that the EU and national measures do not ensure sufficiently the security of operators, failing to meet the increasingly complex operational challenges. The focus needs to be shifted away from asset protection to a more system-oriented protection, which recognises interdependencies across a range of different sectors. Therefore, on 16 December 2020, the European Commission proposed a revision of the ECI Directive and adopted the proposal for a Directive on the resilience of critical entities (the "CER Directive")(COM (2020) 829 final, addressing the need to reduce the vulnerabilities of the critical entities.

To better tackle hybrid threats, the European Commission published the Joint Framework on countering hybrid threats (JOIN/2016/018 final) on 6 April 2016, which aims to facilitate a holistic approach to enable the EU and Member States to counter threats of a hybrid nature by creating synergies between different instruments and fostering close cooperation between all relevant actors (European Commission 2016).

The Joint Framework (JOIN/2016/018 final), states that measures to counter hybrid threats relate to national security and defence, and the primary responsibility lies with Member States, as most national vulnerabilities are country-specific (European Commission 2016, JOIN/2016/018 final). However, since many Member States face common threats, they can be more effectively addressed at the EU level, with the EU functioning as a platform to boost national efforts and, through its regulatory capacity, establish common benchmarks that can help raise the level of protection and resilience across the EU.

According to the European Commission (2016), a crucial step to achieving intelligence and information sharing to prevent and respond to hybrid threats effectively and it is paramount to enhance the resilience of societies and CI (European Commission 2016).

In this context, the EU can play an important role in building Member States' resilience to hybrid threats, and in preventing, responding to, and recovering from crisis (European Commission 2016). The Joint Framework (JOIN/2016/018 final) builds on the European Agenda on Security as well as on sectorial strategies such as EU Cyber Security Strategy, the Energy Security Strategy, and the European Union Maritime Security Strategy. The Joint Framework brings together existing policies and proposes twenty-two operational actions to building resilience by addressing potential strategic and critical sectors such as cybersecurity, critical infrastructures (Energy, Transport, Space), protection of the financial system from illicit use, protection of public health, and supporting efforts to counter violent extremism and radicalization, among others, to build resilience against hybrid threats (European Commission 2016, JOIN/2016/018 final).

4. The new CER Directive (COM (2020)829 final) to improve CI protection

The European Commission's proposal for a revision of the European Critical Infrastructure Directive 2008/114/EC, "Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities" COM(2020) 829 final, (COM (2020) 829 final), represents the Commission's response to introduce complementary efforts to counter hybrid threats and to enhance resilience (COM (2020) 829 final). The proposal covers eleven sectors including energy and transport, banking, financial market

infrastructures, drinking water, wastewater, digital infrastructure, public administration, space, and food (COM (2020) 829 final). By proposing the Critical Entities Resilience (CER) Directive, the Commission intends to create a comprehensive framework to support EU Member States in ensuring that the critical entities can prevent, resist, absorb and recover from all disruptive incidents (COM (2020) 829 final).

The new rules are expected to strengthen the resilience of critical infrastructure against a range of non-cyber threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies like the recent COVID-19 pandemic. The provisions include the Member States' obligation to have in place a strategy for identifying critical entities and ensuring their resilience and to carry out a national risk assessment accordingly. Critical entities would be required to carry out risk assessments of their own and take appropriate technical and organisational measures to boost resilience, and report incidents to the national authorities (COM (2020) 829 final). The Commission offers different forms of support to Member States and critical entities, including risk overview at EU level, best practices, methodologies, cross-border training activities and exercises to test the resilience of critical entities (European Commission 2020). The proposed comprehensive legislative framework also covers the resilience of the transport sector. The Commission will adopt non-binding guidelines to further specify the technical, security and organisational measures that can be taken, including cooperation among two or more Member States, when they have critical entities that are connected in some way or when the critical entity identified in one Member State provides essential services to or in other Member States (European Commission 2020).

On 28 June 2022, the Council presidency and the European Parliament reached political agreement on the proposal to strengthen the resilience of critical entities on 16 September 2022, the final compromise text between the Council and the Parliament was published (COM (2020) 829 final, 2020/0365 COD).

A key element of the compromise was the agreement on the threshold to be identified as critical entity of European significance. The compromise states that an entity will be considered as critical entity of European significance when it provides the same or similar essential services to or in six or more Member States ((COM (2020) 829 final, 2020/0365 COD).

In September 2020, the Commission also presented a proposal for a Digital Operational Resilience Act (DORA), which will strengthen the IT security of financial entities such as banks, insurance companies and investment firms. It aims to make sure the financial sector in Europe is able to maintain resilient operations through a severe operational disruption. The Council and the Parliament reached an agreement on this proposal in May 2022 (European Commission 2020).

In parallel, the Commission also adopted a proposal for a revised Network and Information Systems Directive (NIS2), which aims to ensure robust cyber resilience on the part of a large number of entities (COM(2020) 823 final). The proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap. It proposes to strengthen resilience and preparedness by requiring organisations, including those in the transport sector, to put in place business continuity and crisis management measures. To ensure alignment between the two instruments, all critical entities identified under the CER Directive would be subject to cyber resilience obligations under NIS2 (European Commission 2020).

The NIS 2 Directive strengthens security requirements with a list of focused measures including incident response and crisis management,

vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption. The NIS 2 Directive also contains an expanded scope of sectors and services, including public electronic communication networks or services, digital services such as social networking services, platforms and data centre services, wastewater and waste management, space, manufacturing of certain critical products (including pharmaceuticals, medical devices, chemicals), postal and courier services, food, and public administration (COM(2020) 823 final). Although the EU has taken steps to strengthen its resilience to hybrid threats and to better secure critical infrastructure, the latest attacks on the gas pipelines underline the vulnerabilities and the need to better secure these infrastructures.

5. The fourth Progress Report on the implementation of the European Security Union Strategy

The European Security Union was first introduced in 2016 and aims to ensure that EU security policy reflects the changing threats landscape, to build long-term, sustainable resilience, to engage the EU institutions and agencies, governments, the private sector, and individuals, and to bring together the many policy areas with a direct impact on security (European Commission n.d.). The EU Security Union Strategy covers the period from 2020 to 2025 and focuses on priority areas where the EU can help Member States in fostering security for all those living in Europe. The European Commission regularly presents progress reports on the implementation on the EU Security Union Strategy. On 25 May 2022, the European Commission presented the Fourth Progress Report on the implementation of the EU Security Union Strategy COM(2022) 252 final.

Since the European security threat landscape has dramatically changed in a new context of the Russian war in Ukraine, the fourth Report provides an overview of actions taken on all Security Union to see whether the EU is able to adapt, even in the face of exceptional and unexpected threats (COM(2022) 252 final).

The Russian war of aggression against Ukraine currently dominates the EU security agenda as it not only threatens Ukraine, but it also seeks to damage global stability and security. There are new uncertainties over supplies of energy and other raw materials, and critical infrastructure may be targeted in cyberattacks. Furthermore, the EU's internal safety and security are jeopardised by potential attacks or accidents resulting from chemical, biological, radiological, or chemical agents in the war zone (COM/2022/252 final). The EU has stepped up vigilance and coordination with increased monitoring of the threat landscape and has worked to strengthen resilience to ensure preparedness, according to the Fourth Progress Report.

In the Versailles Declaration of 10-11 March 2022, European leaders stressed the need to prepare for fast-emerging challenges, including by "protecting ourselves against ever-growing hybrid warfare, strengthening our cyber-resilience, protecting our infrastructure - particularly our critical infrastructure - and fighting disinformation" (European Council 2022). The Declaration also mentions that the EU needs to protecting itself against hybrid warfare, strengthening cyber-resilience, protecting the EU's infrastructure and in particular the critical infrastructure, as well as fighting disinformation, among others (European Council 2022). The threats arising from the war underline the need to build a culture of sharing information and expertise between the EU, the Member States, and across the cybersecurity communities. This includes building an integrated situational awareness, shared by the EU institutions, bodies and agencies and Member States (COM/2022/252 final). Regarding vigilance and coordination between the EU and its Member States, the

monitoring of the cybersecurity situation has increased since the Russian war against Ukraine started (COM/2022/252 final). The EU Agency for Cybersecurity (ENISA), the European Cybercrime Centre of Europol and CERT-EU, the Computer Emergency Response Team for EU Institutions, Bodies and Agencies and the EU Intelligence and Situation Centre (EU INTCEN), all contribute to the EU's shared situational awareness, and they provide regular monitoring of suspicious cyber activity, including in specific sectors such as energy, transport and aviation, and have provided assessments to guide preventive action (COM (2022) 252 final).

Already the Fourth Progress Report on the implementation of the EU Security Union Strategy mentions the increased risk that the EU's critical infrastructures and entities might be exposed to an increased level of physical risks, such as sabotage by the state or by state-sponsored actors as part of possible retaliatory measures against the EU. Therefore, the vigilance by EU Member States, EEAS and the Commission services concerning the exposure of critical infrastructures to non-cyber, physical threats is intensified (COM/2022/252 final). Efforts to step up preparedness includes several direct actions, like exercises, guidance, legislative measures, increasing resilience in critical sectors, and work with partners (COM/2022/252 final).

The French Presidency of the Council of the European Union, together with the European External Action Service (EEAS) and the European Union Agency for Cybersecurity (ENISA) organised a scenario-based exercise in early 2022, with the aim of raising awareness at the political level and strengthening cooperation between the operational and political levels in case of a large-scale cyber-attack (COM/2022/252 final).

The Commission also proposed new rules to establish common cybersecurity and information security measures across the EU Institutions, Bodies and Agencies (EUIBA) on 22 March 2022, which are expected to improve the EU administration's resilience and ability to respond to cyber threats and incidents COM/2022/252 final. The security of the EU's energy supply is critical, and the current situation has highlighted the need for clear rules on cyber security. Since Russia's war of aggression against Ukraine started, the objectives intended for the network code on cybersecurity are even more relevant (COM/2022/252 final). The emergency synchronization of the electricity grids of Ukraine and Moldova with the Continental Europe Grid took place in March 2022 after the adoption of risk mitigating measures, notably in terms of cybersecurity (COM/2022/252 final).

The Fourth Progress Report on the Security Union Strategy concludes that the EU can adapt to exceptional and unexpected threats such as from Russia's war of aggression against Ukraine, and that a determined implementation of the Security Union Strategy is more important than ever (COM/2022/252 final).

6. Measures to strengthen preparedness and resilience of the EU transport sector: The contingency plan for transport

In the past, several terrorist attacks or attempts were aimed at the EU's transport system, and transport is an effective target due to the large number of people who use it daily. During the COVID-19 pandemic, telecommunications, including 3G/4G/5G infrastructure (e.g., repeaters, repeater bridges and cell towers) and other network components (e.g., relays and cables) were also targeted. In July 2021, also natural disasters like floods in Belgium and Germany caused many deaths and severe, long-lasting disruption to transport. (COM (2022) 211 final)

While the full effect of Russia's military aggression against Ukraine is yet to unfold, Member State authorities and EU transport

companies recognise that the critical infrastructure needs more vigilance (COM (2022) 211 final).The Russian war and the EU's sanctions as a reaction on it have also created many challenges for EU transport, from safety risks for EU civil aviation and truck drivers stuck in conflict zones, to the destruction of Ukrainian transport infrastructure, and cutting off supply chains and threatening global food security among others. Critical infrastructures and entities that operate them may also be exposed to physical risks, such as sabotage by the state or by state-sponsored actors as part of possible retaliatory measures against the EU (COM/2022/252 final). Therefore, the threats arising from the war underline the need to build a culture of sharing information and expertise between the EU, the Member States, and across the cybersecurity communities, also beyond cyber security, as CI is also exposed to non-cyber, physical threats, and the smooth functioning of the internal market depends on the functioning of the transport infrastructure (COM (2022) 252).

Therefore, the Commission has been working to strengthen the preparedness and resilience of the EU transport sector, based on a new Contingency plan for transport (COM/2022/211 final), which was adopted on 23 May 2022. It draws lessons from both the COVID-19 pandemic and Russia's military aggression against Ukraine and proposes a toolbox of 10 actions to guide the EU and its Member States. It also highlights the importance of regular resilience testing for different crisis scenarios, bringing together relevant EU agencies or other actors, and building on existing processes (COM/2022/211 final). The new Contingency plan for transport (COM (2022) 211 final) intends to prepare for and respond to major events, in addition to other relevant EU principles. The toolbox of 10 actions to guide the EU and its Member States when introducing emergency crisis-response measures. It includes ensuring minimum connectivity, building cyber and hybrid threats resilience and enhances cooperation with international partners on crisis preparedness and response. It also highlights the importance of regular resilience testing for different crisis scenarios, bringing together relevant EU agencies or other actors, while building on existing processes (COM/2022/211 final). The toolbox measures range from a longer-term preparatory actions to tools that can be used for an immediate measures (COM (2022) 211 final). The common objective is to be better prepared for a swift response to any accident or event capable of causing severe disruption such as natural disasters, pandemics, terrorist attacks, cyberattacks, ransomware, military conflicts, infrastructure failure (such as bridge or tunnel collapses), or power outages (COM (2022) 211 final). Moreover, the Commission continues to work with the International Civil Aviation Organization (ICAO), EUROCONTROL and International Maritime Organization (IMO) on preventive cybersecurity measures, among others (COM (2022) 211 final)

The Commission will actively support the preparedness to a crisis situation also in cooperation with the EU agencies, by coordinating and maintaining regular discussions with international partners among others (COM (2022) 211 final). The Commission calls on the European Parliament and the Council to fully engage in the legislative work to strengthen the EU transport sector's resilience and to finalising the work on the pending proposals on TEN-T, Intelligent Transport Systems, Single European Sky, ReFuelEU Aviation, FuelEU Maritime, and the Alternative Fuel Infrastructure Regulation to build up long-term resilience in EU transport (COM (2022) 211 final).

7. Conclusion

Russia's war against Ukraine is deeply affecting the EU transport system and the security of critical infrastructures. Rising oil and gas

prices, broken supply chains, closure of skies and markets, and potential and actual sabotage action against the EU's critical infrastructure marks the new reality of increased hybrid warfare activities in Europe while the Russian war in Ukraine continues. While the responsible for the attack against the gas pipelines in the Baltic Sea NS 1 and NS 2 is still unknown, the tactical disruption might best suit Russia's political and revenue aims, although Russia rejects any connection to the attacks on the pipelines.

While investigations into the NS 1 and NS 2 leaks are still ongoing, already on 8 October 2022, some acts of sabotage against the German railway company Deutsche Bahn occurred, underlining that a period of further incidents of hybrid warfare seems to be only starting. The number of hybrid attacks could further rise, as the war continues, which adds to the still existing challenges of the COVID-19 pandemic.

After the latest attacks against the gas pipelines, there is no doubt that the EU's CI needs to be better protected against an increasing number of cyber threats, hybrid attacks or sabotage. There is a need to improve how critical infrastructure is secured, as there exist all kinds of valuable targets for the aggressor, from roads to bridges, to hospitals, to supply lines.

The level of preparedness can and should be stepped up and prevention and preparedness initiatives need to be introduced. There is a need to continue enhancing and reinforcing early warning systems for actionable information to allow for informed decision-making. The Commission can be expected to support Member States to improve their crisis preparedness. The threats arising from the war underline the need to build a culture of sharing information and expertise between the EU, the Member States, and also at international level. This cooperation and information exchange needs to become a routine as it would help to inform authorities and could thereby help to prevent incidents of hybrid warfare or cyberattacks.

The general focus needs to be shifted away from asset protection because the vast array of CI targets in the EU might never be fully defensible. It will need a more system-oriented protection and vigilance, which recognises interdependencies across a range of different sectors.

However, since hybrid attacks are more difficult to prevent or respond to, it remains to be seen if and in how far the EU and its Member States can take measures to make CI and in particular the transport system infrastructure more prepared and resilient against hybrid attacks.

References

COM(2006) 786 final: COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection. In: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF, Brussels, 12.12.2006

COM (2020) 829 final, 2020/0365 COD: Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities (First reading) - Confirmation of the final compromise text with a view to agreement. COM (2020) 829 final, 2020/0365 COD. In: https://data.consilium.europa.eu/doc/document/ST-12414-2022-INIT/en/pdf, 16 December 2020, accessed 7 October 2022

COM/2022/211 final) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A contingency plan for transport. COM/2022/211 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A211%3AFIN, 23 May 2022

COM/2022/211 final: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A

contingency plan for transport. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A211%3AFIN, 23 May 2022, accessed 10 October 2022.

COM(2022) 252 final: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Fourth Progress Report on the implementation of the EU Security Union Strategy. COM(2022) 252 final. In: https://ec.europa.eu/info/sites/default/files/communication_fourth_progress_report-eu_security_union_strategy.pdf, Brussels, 25.5.2022

Council Directive 2008/114/EC: Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, 23.12.2008, accessed 7 October 2022

Council of the EU (2022a): Declaration by the High Representative on behalf of the European Union on leaks in the Nord Stream gas pipelines. In: https://www.consilium.europa.eu/en/press/press-releases/2022/09/28/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-leaks-in-the-nord-stream-gas-pipelines/, 28 September 2022, accessed 5 October 2022

Council of the European Union, General Secretariat of the Council (2022): Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities (First reading)
– Confirmation of the final compromise text with a view to agreement. Interinstitutional File: 2020/0365(COD). In: https://data.consilium.europa.eu/doc/document/ST-12414-2022-INIT/en/pdf, 16 September 2022, accessed 7 October 2022

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) (n.d.): Hybrid threats as a concept. In: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/, no date, accessed 4 October 2022

European Commission (n.d.): European Security Union. In: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en, no date, accessed 10 October 2022

European Commission (2016): FAQ: Joint Framework on countering hybrid threats. In: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250, 6 April 2016, accessed 7 October 2022

European Commission (2020): The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU. In: https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en, 16 December 2020, accessed 5 October 2022

European Commission, Migration and Home Affairs (2022a): Enhancing the resilience of Europe's critical entities against attacks and natural hazards. In: https://home-affairs.ec.europa.eu/news/enhancing-resilience-europes-critical-entities-against-attacks-and-natural-hazards-2022-06-30_en, accessed 5 October 2022

European Commission (2022b): Security Union: Commission welcomes today's political agreement on new rules to enhance the resilience of critical entities. In: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4157, 28 June 2022, accessed 4 October 2022

Government offices of Sweden: Likely deliberate act behind leaks in Nord Stream 1 and 2 Baltic Sea gas pipelines. In: https://www.government.se/articles/2022/09/likel

y-deliberate-act-behind-leaks-in-nord-stream-1-and-2-baltic-sea-gas-pipelines/, 28 September 2022, accessed 5 October 2022

Hoffmann, Carsten: Neues Führungskommando - hybride Angriffe gelten als „worst case“. In: https://www.dbwv.de/aktuelle-themen/blickpunkt/beitrag/neues-fuehrungskommando-hybride-angriffe-gelten-als-worst-case, 25.09.2022

JOIN/2016/018 final: JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018, 6.4.2016, accessed 5 October 2022

Kalniete, Sandra and Tomass Pildegovičs (2021): Strengthening the EU's resilience to hybrid threats. Wilfried Martens Centre for European Studies. In: https://www.martenscentre.eu/wp-content/uploads/2021/07/4.pdf, European View 2021, Vol. 20(1) 23-33, accessed 7 October 2022