Intelligence Law and Policies in Europe

Dietrich / Sule

2019
ISBN 978-3-406-69455-4
C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.
beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Regional organisations also play an active role in the field of critical information infrastructure protection. In 2008 OECD adopted the Recommendation of the Council on the Protection of Critical Information Infrastructures, calling for the member states to implement such measures as risk management strategies, creation of CERT (computer emergency response teams) and CSIRTs (computer security incident response teams), public-private partnerships and others[87]. The European Union created the European Network and Information Security Agency (ENISA) in 2004 for coordination of efforts among Member States, launched the EU Cybersecurity strategy in 2013, and subsequently adopted the Directive on security of network and information systems (NIS Directive) in 2016.[88] The possible effect of NIS Directive is, however, still unknown, as the Member States should identify the operators of essential services that are regulated by the Directive by 9 November 2018[89]. **45**

3. Frameworks for cyberwar and warfare

There is no international consensus on the thresholds and triggers for malicious activity in cyberspace to reach the level of threat or use of force, threat to the peace, breach of the peace or act of aggression, or armed attack as stipulated by the UN Charter and humanitarian law.[90] Undoubtedly, as many state-supported threats in cyberspace fall below such a threshold, it is uncertain which rules should apply and how to prevent states from supporting cyberattacks. The development of frameworks in this area considers, firstly, the application of the law on the use of force (ius ad bellum) and international humanitarian law (ius in bello) to cyberspace[91], and, secondly, the rules for responsible state behaviour. On the national level and on the level of military alliances cyberwar constitutes the development of military strategies and offensive and defensive capabilities of the nation states. **46**

The question of applying international humanitarian law (ius in bello) to acts and conflicts in cyberspace and the issue of responsible state behaviour have been addressed, most prominently, on the level of the United Nations in the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE).[92] The group, which started its work in 2004, produced three consensus reports: in 2010, 2013 and 2015. Two of the reports – in 2013 and 2015 – showed some agreement on the legal matters related to applicability of international law to cyberspace and responsible behaviour of states, such as not interfering with each other's critical infrastructures, not targeting each other's computer emergency response teams, assistance in investigation of cyberattacks and responsibility for actions originating from countries' territory.[93] **47**

beck-shop.de
DIE FACHBUCHHANDLUNG

[87] OECD, *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*, 2008, available at: http://www.oecd.org/sti/40825404.pdf.

[88] EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[89] Art. 5 of EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[90] Lotrionte, in: Beck (ed.), *Law and Disciplinarity. Thinking Beyond Borders*, 2013, 67 (71); Pipyros et al, A new strategy for improving cyberattacks evaluation in the context of Tallinn Manual, *Computers & Security* 74 (2017), 371 (375).

[91] Giles, 2017, above fn. 63, 9.

[92] See e.g. Tikk-Ringas, *Georgetown Journal of International Affairs* 17.3 (2016), 47 et seq.

[93] United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2013, available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98; United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2015, available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

48 However, the 5th GGE (with the mandate 2016–2017) after two years of work "collapsed"[94] as the final report was rejected by a number of countries, including Cuba and, allegedly, Russia and China[95] due to their disagreement with the inclusion of such provisions as the right to self-defence, the right to respond to wrongful acts and the applicability of the international humanitarian law into the report.[96] It is currently unclear whether the United Nations will continue the process of norm-making in this field in GGE format or in any other way. Undoubtedly, the failure of the 5th GGE shows the divergence in the legal and political debates and the inability of the UN to resolve these issues in the foreseeable future.

49 Further frameworks related to military activities in cyberspace can be found on the level of military alliances, notably, NATO.[97] The first attempts to evolve cyber capabilities were taken at the NATO Summit in 2012 and followed by the creation of the NATO Computer Incident Response Capability. In 2005, NATO included the cyber threat in the Comprehensive Political Guidance document. The need to establish cyber capabilities was fully recognised after attacks against Estonia in 2007 and led to the adoption of the Policy on Cyber Defence.[98] In 2014 the Wales Summit affirmed that "cyber-defence is part of NATO's core task of collective defence". Furthermore, cyberspace was recognised as a "domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea" at the NATO meeting in Warsaw in 2016.[99]

50 Current NATO's strategy for cyber defence includes the implementation of national cyber defence capabilities in NATO member countries via the NATO Defence Planning Process, integration of cyber defence into Smart Defence initiatives via creation of the Malware Information Sharing Platform, the Smart Defence Multinational Cyber Defence Capability Development project, the Multinational Cyber Defence Education and Training project,[100] and cyber defence exercises with NATO member countries[101] In 2015 NATO also developed the Memorandum of Understanding on Cyber Defence, which is aimed to increase situational awareness. For research, training and capacity building NATO established the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia, as a research and educational enterprise not formally part of

beck-shop.de
DIE FACHBUCHHANDLUNG

[94] Schmitt/Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, Friday, 2017, available at: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/; see also Markoff, *Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2017, available at: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm; Segal, *The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?,* 2017, available at: https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

[95] Korzak, *UN GGE on Cybersecurity: The End of an Era?*, 2017, available at: http://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe.

[96] Schmitt/Vihul, 2017, above n. 94.

[97] See for more details: Veenendaal/Kaska/Brangetto, *Is NATO Ready to Cross the Rubicon on Cyber Defence?* Cyber Policy Brief, available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf; Lewis, *The Role of Offensive Cyber Operations in NATO's Collective Defence*, 2015, available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf; Pernik, *Improving Cyber Security: NATO and the EU*, 2014, available at: https://www.icds.ee/fileadmin/media/icds.ee/failid/Piret_Pernik_-_Improving_Cyber_Security.pdf. See also Masala/Scheffler Corvaja, chapter xx, mn. xxx.

[98] Fidler/Pregent/Vandurme, *NATO, Cyber Defense, and International Law*, 2013, available at: http://www.repository.law.indiana.edu/facpub/1672.

[99] See www.nato.int/cyberdefence/.

[100] See http://www.nato.int/cps/en/natohq/topics_78170.htm.

[101] See: Krause, *NATO on its Way Towards a Comfort Zone in Cyber Defence*, 2014, 5, available at: http://www.ccdcoe.com/sites/default/files/multimedia/pdf/TP_03.pdf.

NATO but supported by NATO member countries and several NATO schools and colleges. Furthermore, in 2016 NATO also signed the Technical Arrangement on cyber defence cooperation with the European Union[102].

One of the results of NATO's involvement in the cyber domain is the development of the Tallinn Manual on the International Law applicable to cyber warfare. The Tallinn manual is a project initiated by NATO and carried out by a group of experts, which consisted of practitioners and academics from NATO member countries. The Manual, first published in 2012, represents an "academic, nonbinding study"[103] aimed to consider how the existing public international law is applicable to cyberspace rather than creation of any new norms applicable to cyberwar or cyberwarfare.[104] The second version of the manual – Tallinn Manual 2.0 was released in 2017 and includes, in addition to the previous study, a legal analysis of the common cyber incidents.[105] **51**

While it is clear that the Tallinn manual represents a significant step forward to fill the gaps in cyber-norms and to reach consensus among the experts on the applicability of the international law to cyberspace,[106] it has some drawbacks in terms of possible influence. The critics of Tallinn manual point out that it lacked the wider representation of nation states in its development[107] and as a non-state initiative lacks the power of norm-making or norm interpretation process.[108] Moreover, from a substantive point of view, the manual was criticised for possibly lowering the threshold for the applicability of the right to self-defence for non-state actors together with dropping the threshold of the definition of armed attack, and, therefore, increasing potential of the use of force and changing the landscape of the possible conflicts in the future.[109] Nevertheless, in the context of failure of UN GGE in 2017, the potential influence of the manual is unclear. **52**

While the discussion on cyberwarfare and applicability of the international law is getting fragmented, nation states started implementing cyberwarfare capabilities in their military doctrines. It is hard to assess exactly how many states are developing or planning to develop offensive cyberwarfare capabilities and at which stage this process finds itself at the moment. According to the joint statement by Clapper, Lettre and Rogers, "as of late 2016" at least 30 states "are developing offensive cyberattack capabilities".[110] The UNIDIR report of 2011, which was using open-source information from 133 states, found out that at least 33 countries included cyberwarfare in their military doctrines, planning or organisation.[111] As it will be further discussed in the Part D.V., in the European Union there are several states which openly develop cyberwarfare capabilities. **53**

beck-shop.de
DIE FACHBUCHHANDLUNG

[102] NATO, 2016, *NATO and the European Union enhance cyber defence cooperation*, available at: https://www.nato.int/cps/en/natohq/news_127836.htm.

[103] Lotrionte, 2013, above n. 90, 69.

[104] See e. g. Barnsby/Reeves, in *Texas Law Review* 95.7, 2017, p. 1515 (1515 et seq.).

[105] Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017.

[106] Neutze/Nicholas, *Georgetown Journal of International Affairs*: *International Engagement on Cyber*, 2013, 3 (9 et seq.).

[107] McGhee, *Journal of Law and Cyber Warfare,* 2/2013, 64 (103).

[108] Mačák, 2016, above fn 62, 136.

[109] Boulos, in: Ramírez/García-Segura (eds.), *Cyberspace. Advanced Sciences and Technologies for Security Applications*, 2017, 231 (241).

[110] Clapper/Lettre/Rogers, *Joint Statement for the record to the Senate Armed Service Committee. Foreign Cyber Threats to the United States*, 2017, 5, available at: https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

[111] Lewis/Timlin, *Cybersecurity and Cyberwarfare*, 2011, 3, available at: http://unidir.org/publications.

4. Other regimes

54 Other regimes in addressing cybersecurity threats include confidence building measures, public-private cooperation, technical and organisational measures and capacity building.

55 – *Confidence building measures* represent normative commitments that states are supposed to respect. Such commitments focus on preventing and reducing the risk of state conflicts or outbreak by mitigating mistrust, misunderstanding and miscalculations via exchange of information, resources, increasing awareness and facilitating common understanding.[112] Sets of confidence building measures have been developed mostly on the regional levels by the organisations such as OSCE, AOS, ASEAN, SCO and others.[113]

56 – *Public-private cooperation* is considered important due to the significant role of the private sector in managing critical information infrastructure and networks and "existence of myriad actors in the information security field".[114] The scope and scale of public-private collaboration in cybersecurity involves different areas of ICT markets and various forms of cooperation: from ad hoc to long-term public-private partnerships and nationwide joint cybersecurity initiatives.[115]

57 – *Technical and organisational measures*, such as risk analysis, training, control and certification, alert systems and recovery strategies have become the core of organisational cybersecurity policies for both industrial control systems and other actors in the private sector.[116]

58 – *Capacity building* frameworks address the vulnerabilities of cross-border externalities[117] because the lack of cybersecurity capacity in one country can pose significant risks on another. The programs for capacity building include the initiatives from international and regional organisations such as ITU[118], EU[119], OAS[120], and private sector and academia's efforts such as Oxford University Global Cyber Security Capacity Centre and Microsoft's capacity building programs.[121] Furthermore, the Global Forum

beck-shop.de
DIE FACHBUCHHANDLUNG

[112] Trimintzios et al, *Cybersecurity in the EU Common Security and Defence Policy (CSDP),* 2017, 19, available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf; Ziolkowski, in: Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, 2013, 533 et seq.; Lewis, *Disarmament Forum* 4/2011, 53 et seq.

[113] See Giles, 2017, above n. 63, xiv et seq.; Ott, *Fletcher Security Review* 3.1 (2017), 67 (70).

[114] Brown/Snower, *Global Economic Solutions 2010/2011*, Global Economic Symposium, 2011, 143, available at: https://www.global-ecnomic-symposium.org/solutions/publications/global-economic-solutions/global-economic-solutions-2010-11.

[115] Tropina, 2015, above n. 58, 20 et seq.

[116] See Agence Nationale de la Sécurité des Systèmes d'Information, *Managing Cybersecurity for Industrial Control Systems,* 2014, 16 et seq., available at: https://www.ssi.gouv.fr/uploads/2014/01/Managing_Cybe_for_ICS_EN.pdf, Stouffer, *Guide to Industrial Control Systems Security*, 2015, 3-1 et seq, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf; Luiijf/te Paske, Cyber Security of Industrial Control Systems. 2015, 35 et seq., available at: http://publications.tno.nl/publication/34616507/KkrxeU/luiijf-2015-cyber.pdf.

[117] Global Public Policy Institute, *Advancing Cybersecurity Capacity Building*, 2017, 1, available at: http://www.gppi.net/publications/.

[118] See http://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity_metrics_capacity_building.aspx; Obiso, *Cybersecurity: Capacity Building and Emergency Response*, 2014, available at: https://itu4u.wordpress.com/2014/05/27/cybersecurity-capacity-building-and-emergency-response/.

[119] European Commission, *EU cybersecurity initiatives*, 2017, available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

[120] OAS, *American States' Inter-American Integral Strategy to Combat Threats to Cyber Security*, 3 et seq., available at: https://www.oas.org/juridico/english/cyb_pry_strategy.pdf.

[121] Muller, *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*, NUPI Report, no. 3 2015, 8, available at: https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf.

for Cyber Expertise (GFCE) was created in 2015 as a global capacity building initiative between governments and private stakeholders.

D. Cybersecurity and Cyber Intelligence

I. Reactive and proactive approaches

The nation states are increasingly recognising cyberspace as a new warfare domain, and are therefore developing offensive and defensive capabilities to address constantly evolving cyber threats.[122] However, while the technical capabilities of the attackers and defenders might evolve in parallel, many cybersecurity approaches are still rather static and reactive: they aim to identify the intrusion, minimise the disruption and mitigate the consequences after the malicious actors are "already inside the wire".[123] While investment into technology is essential, it cannot be effective on its own anymore due to the growing proliferation of adversaries, the increasing complexity of cyber-threats, the lack of legal frameworks, be it on national or international level, and the challenge of attribution.[124] **59**

Any malicious activity in cyberspace has a human interaction behind it. It is the motivation of the attacker that brings acts of adversaries to one or another domain – be it military defence or criminal justice. Serious persistent threats and attacks require adversaries to plan them, to collect information, to determine the targets, to acquire the access to the network. This planning process takes time, therefore it is important to empower policy-makers with the knowledge about adversaries' capabilities and potential actions and use this time to develop solutions for an intelligence-based defence.[125] There is already a recognition that cyber defence shall not follow only a passive, reactive approach. It is not enough to ensure the development of legal and technical instruments to address threats in cyberspace and building technical capability to react to the incidents that already happened. Therefore, some nation states are increasingly embracing the concept of intelligence-driven cyber defence,[126] where intelligence, as in case of any complex security threats, is a central component. The aim of intelligence-driven cyber defence is to assess the range of geopolitical, cultural, social and other contexts that influence decision-makers behind the attack.[127] This approach broadens the focus from the use of technology for identification and elimination of attacks and intrusions to a wider set of actions. Intelligence-driven cyber defence aims to collect information from expanded sources about adversaries and their capabilities, objectives, doctrines and limitations in order to understand the motivations behind malicious activities and prevent and anticipate cyber-incidents. **60**

beck-shop.de
DIE FACHBUCHHANDLUNG

[122] Gehem et al., *Assessing Cyber Security*, 2015, 49, available at: https://hcss.nl/report/assessing-cyber-security/.

[123] Mattern et al., *International Journal of Intelligence and Counterintelligence* 27.4 (2014), 702 (705); see also Intelligence and National Security Alliance, *Operational Levels of Cyber Intelligence*, 2013, 3, available at: https://www.insaonline.org/resources/publications/; Borum et al., *The Coast Guard Proceedings* 71.4 (2014–2015), 65 (67); Nielsen, *Orbis* 56.3 (2012), 336 (349).

[124] Borum et al., *Information & Computer Security* 23.3 (2015), 317 (329).

[125] Intelligence and National Security Alliance, 2013, above fn 123, 4 et seq.

[126] See D.V. for national approaches within Europe.

[127] Brantly, *The Decision to Attack*, 2016, 119 et seq.

61 There is also an increasing discussion to what extent offensive capabilities by launching a counterstrike to the supposed source of an attack can and should be considered in the development of proactive approaches to maintain cybersecurity. These activities are discussed under the term "hack back" and reach from accessing systems to delete stolen content to DDoS attacks on networks with the intent to shut down the adversary's systems.[128] The latter example illustrates that these countermeasures can overlap with the issues that are discussed in the context of cyberwar. This especially relates to the state's right to self-defence, the issue of attribution of the attack and the intensity of the counterattack.[129]

II. Intelligence in cyber domain or "cyber intelligence"?

62 Although there is no agreed definition of cyber intelligence,[130] it can generally be described as information collection about, comprehensive assessment of and reaction to the adversarial activities, capabilities and intentions in the cyber domain for intelligence purposes.[131] It relies on data collected from a wide range of traditional intelligence sources (like human intelligence, open source intelligence and signal intelligence) with the aim to inform policy-makers at any level of the cyber domain.

63 Cyber intelligence should be distinguished from a broader concept of using information and communication networks as a source for collecting intelligence, where digital developments and information gathering supplement traditional tools for data collection.[132] While traditional intelligence is also facing challenges related to cyberspace as the new environment for operations and is struggling with the consequences of the information revolution,[133] cyber intelligence, as a distinct field, operates with the aim to address cybersecurity threats, including threats to national security. Furthermore, in addition to a general process of collecting information to address cyber threats, cyber counter-intelligence, as part of a broader concept of cyber intelligence, focuses on countering the intelligence actions of the adversary; this includes detection, deterrence, prevention, degradation, exploitation and neutralisation of the foreign intelligence services' operations related to all the sceptre of possible threats – from cyberwarfare to their efforts to collect information.[134]

64 Both cyber intelligence and counter-intelligence require new sources and means of gathering information. This is especially true in such areas as cyber defence due to the fact that unlike the conventional weapons cyber-weapons are available to a wide range of actors as they require less infrastructure and no restricted, controlled or limited-supply materials, and therefore, tracing such processes is harder and requires more information collected from different sources.[135]

beck-shop.de DIE FACHBUCHHANDLUNG

[128] See e.g. Kesan/Hayes, *Harvard Journal of Law & Technology* 25.2, 431 (474 et seq.); see also below n. 182.

[129] On these issues see Tsagourias, *Journal of Conflict and Security Law* 17.2 (2012), 229 et seq.

[130] See Uthoff, in: Lemieux (ed.), *Current and Emerging Trends in Cyber Operations*, 2015, 199 et seq.

[131] Intelligence and National Security Alliance, *Tactical Cyber Intelligence*, 2015, 1, available at: https://www.insaonline.org/resources/publications/.

[132] See e.g. how the digital and cyber developments impact HUMINT: Gioe, in: Dover/Dylan/Goodman (eds.), *The Palgrave Handbook of Security, Risk and Intelligence*, 2017, 213.

[133] See e.g. Degaut, *Intelligence and National Security* 31.4 (2016), 509 et seq.; Dunn Cavelty/Maurer, *Security Dialogue* 40.2 (2009), 128 et seq.

[134] Duvenage/von Solms/Jaquire, Conceptualising Cyber Counterintelligence, *Proceedings of the 15th European conference on Cyber Warfare and Security*, 2016, 93 (96 et seq.).

[135] Williams/Shimeall/Dunlevy, *Contemporary Security Policy* 23.2 (2002), 1 (4).

III. Levels and sources of cyber intelligence

Cyber intelligence operates on several levels, which are complementary and supplementary to each other:[136] **65**

On the *strategic* level, cyber intelligence focuses on the long-term issues that can impact strategic decisions.[137] This level aims to provide information for political decision-making, assess the cyber-environment, define the intentions of adversaries that can have an impact on the national cybersecurity and estimate the capability of the malicious actors. It delivers a framework for all other levels of cyber intelligence activities by framing a "concept" for cyberspace operations. **66**

Tactical cyber intelligence is the collection and analysis of data in order to understand the threats and prepare for them.[138] It links the macro-level provided by strategic intelligence with the micro-level of individual cases where tactical intelligence is supposed to respond to the dynamic threats by focussing on day-to-day defensive activity, on "what is happening on the network".[139] The tactical level includes tactics, procedures and tools to methodologically understand the patterns of behaviour or approaches of an adversary and examine the compromise indicators.[140] Strategic and tactical levels are mutually reinforcing as tactical assessment can help strategic analysis.[141] The reactive approaches to cyber threats are usually focussed on the analysis carried out on the tactical level as this level concentrates on the particular events happening on the network. This is exactly why there is a need to shift the focus from tactics to strategy and mutually reinforce both levels because acting on the tactical level mostly means that adversary is either close to getting access to the system or is already inside the network.[142] **67**

beck-shop.de
DIE FACHBUCHHANDLUNG

Operational cyber intelligence bridges the two other levels – strategic and tactical. It refers to collection of specific information that is required to comprehend the operational environment, objectives, trends, resources and activities of adversaries and also to plan and execute cyber operations and achieve strategic goals in the cyber domain.[143] Intelligence analysis at this level can also overlap with investigations of a single case and include the assessment of data related to a particular incident, the identification of specific vulnerabilities that have been exploited, and the analysis related to attribution.[144] **68**

While addressing cyber threats becomes distinct from traditional intelligence and the focus of data collection might shift, the critical aspects of the traditional intelligence cycle model stay the same: direction and requirements, collection of data, processing and exploitation, analysis and production, dissemination, consumption and feedback.[145] **69**

---

[136] In practice, the levels are not always sharply distinguishable. On the corresponding levels of military cyber operations see Herr/Herrick, in: Harrison/Herr, *Cyber Insecurity*, 2016, 259 (266 et seq.).

[137] Uthoff, 2015, above fn 130, 202; Borum et al., above fn 124, 319; Williams/Shimeall/Dunlevy, above fn 135, 9.

[138] Intelligence and National Security Alliance, 2015, above n. 125, 2.

[139] Julisch, Understanding and overcoming cyber security anti-patterns, *Computer Networks* 57.10 (2013), 2206 (2210); See also Williams/Shimeall/Dunlevy, above n. 135, 12; Borum et al., above n. 124, 68.

[140] Uthoff, 2015, above n. 130, 203.

[141] Williams/Shimeall/Dunlevy, 2002, above n. 135, 12.

[142] Intelligence and National Security Alliance, 2013, above n. 125, 10.

[143] Uthoff, 2015, above n. 130, 203.

[144] Williams/Shimeall/Dunlevy, 2002, above n. 135, 12.

[145] On the intelligence cycle in general see Omand, [in this book]; Johnson, in: Johnson (ed.), *The Oxford Handbook of National Security Intelligence*, 2010, 3 (12 et seq.). The intelligence cycle model recently has been criticized as outdated and oversimplified, see Richards, in Phythian (ed.), *Understanding*

However, it is clear that cyber intelligence needs to include all the methods of data collection that traditional intelligence rely on to get as much information about the adversary as possible.[146] Any intelligence discipline can potentially provide data of crucial value for cyber intelligence. This includes collection of data coming from such disciplines as communications intelligence (COMINT), signal intelligence (SIGINT), human intelligence (HUMINT), open source intelligence (OSINT), geospatial and measurement intelligence (GEOINT) as critical components,[147] which are further combined with other sources of data such as unclassified network data and data from CERTs, data about cyber-activity of a particular country or relevant geopolitical events.

IV. Approaches at EU level

70 The EU Member States mainly consider the issue of cybersecurity as their national competence due to the sensitivity of the issue and its connection to national security and defence. However, the understanding of the cross-border nature of threats and growing concerns about the possibility of the vulnerabilities of one Member State to affect others and the entire Union, called for the development of coordinated approaches to cybersecurity in the European Union. This coordination till recently was rather happening in an ad hoc manner, distributed across different domains and institutions.[148] The concrete efforts to shape a comprehensive cybersecurity agenda at EU level started with the harmonisation of approaches to tackling cybercrime, in particular, adoption of the EU Framework decision on attacks against information systems in 2004 (later repealed by the EU Directive on attacks against information systems 2013[149]). However, some critical parts of the overarching cybersecurity approach where the Member States traditionally try to protect their sovereignty, such as cyber defence, were missing until the adoption of EU Cybersecurity Strategy in 2013. The EU Cybersecurity Strategy was further followed by the Directive on security of network and information systems (EU NIS directive) in 2016 and the recent proposal for the creation of the EU Cybersecurity Agency in September 2017.[150]

beck-shop.de
DIE FACHBUCHHANDLUNG

71 The EU Cybersecurity strategy 2013 was the first attempt to address the entire spectrum of cybersecurity threats at EU level, including both, civil aspects of cybersecurity and cyber defence and clearly establish priorities for the cybersecurity policy that previously was spread across different regulatory frameworks. The document identified five strategic priorities, which include achieving overall resilience, fighting cybercrime, developing cyber defence policies and capabilities in relation to the Common Security and Defence Policy (CSDP), developing industrial and technological resources, and establishing a coherent EU cyber diplomacy. The three first tasks were assigned to

---

the Intelligence Cycle, 2013, 43 (46 et seq.); Hulnick, in Phythian (ed.), *Understanding the Intelligence Cycle*, 2013, 149 (152 et seq.). on cyber specific aspects see Brantly, in Phythian (ed.), *Understanding the Intelligence Cycle*, 2013, 76; Williams/Shimeall/Dunlevy, above n. 135, (15 et seq.); Intelligence and National Security Alliance, above n. 131, 6 et seq.

[146] Brantly, in Phythian (ed.), *Understanding the Intelligence Cycle*, 2013, 76 (81). See also Williams/Shimeall/Dunlevy, above fn 135, 15; Davies, *Information, Communication & Society*, 2.2 (1999), 115 (129).

[147] Some authors also identified new categories of intelligence sources in the cyber domain like e.g. social media intelligence (SOCMINT), see Omand/Bartlett/Miller, *Intelligence and National Security Journal* 27.6 (2012), 801 et seq.

[148] Darmois/Schméder, *Cybersecurity: a case for a European approach*, 2016, 11, available at: http://www.securityintransition.org/wp-content/uploads/2016/02/WP11_Cybersecurity_FinalEditedVersion.pdf.

[149] See above n. 78.

[150] European Commission, Press release IP/17/3193 from 19 September 2017.