AUSTRIAN INSTITUTE FOR EUROPEAN AND SECURITY POLICY

Bundesministerium Landesverteidigung

Nr. 2019/2

Cyber- und Informationssicherheit

Zwei Seiten derselben Medaille

von Michael Zinkanell
März 2019

AIES STUDY

Executive Summary

Das folgende Impulspapier wurde im Auftrag des Bundesministeriums für Landesverteidigung (BMLV) verfasst und widmet sich den neuen Dynamiken der Hybriden Bedrohungen sowie erweiterten Gegenmaßnahmen, welche das Jahr 2018 geprägt haben. Durch den intensivierten Einsatz von schädlichen Desinformationskampagnen wurde das Spektrum der Hybriden Bedrohungen um Komponente der gezielten Manipulation, mit dem Ziel das Vertrauen in politische Systeme auszuhöhlen, erweitert. Zudem stieg Ausmaß und Intensität chinesischer Cyberangriffe und digitaler Spionagefälle rasant an, was im Zusammenhang mit dem geplanten Ausbau des 5G-Mobilfunknetzes eine zunehmende Bedrohung der wirtschaftlichen, staatlichen und europäischen Sicherheit darstellt. Auf institutioneller Ebene der EU und der Mitgliedsstaaten kam es zu einer weitgehenden Finalisierung der Strategiedokumente zum Ausbau der Cyber- und Informationssicherheit. Konkrete präventive und reaktive Handlungen sowie ganzheitliche Umsetzungen als Folge auf die entwickelten Strategien sind in den meisten Fällen noch ausständig. All dies ist Indiz dafür, dass jene neue fluide Bedrohungslage langfristig andauern wird und sich in ständigem Wandel befindet. Daher muss eine konstante Evaluierung derzeitiger sowie Weiterentwicklung neuer strategischer und operativer Gegenmaßnahmen forciert werden.

Inhaltsverzeichnis

1. Einleitung

Die Erkenntnisse aus der jüngsten Vergangenheit über die Instrumente und Intensität hybrider Kriegsführung ermöglichten einen Einblick in den Facettenreichtum an Einsatzmöglichkeiten und Auswirkungen jener neuartigen Form der Bedrohung. Innerhalb der letzten Jahre kam es nicht nur zu einem deutlichen Anstieg der Formen und Fälle hybrider Angriffe, sondern auch zu einer Intensivierung der Durchführbarkeit und Folgewirkung. Heute, in Zeiten in denen digitale Netzwerk-, Kommunikations- und Informationssysteme das Rückgrat des ökonomischen Aufschwungs darstellen und Schlüsselsektoren wie Gesundheit, Transport, Wissenschaft und Energie auf digitale Infrastruktur angewiesen sind, liegt die Fragilität und Vulnerabilität der sozialen, wirtschaftlichen und politischen Ordnung einer digitalen Abhängigkeit zugrunde.

Jene neue Art der Bedrohungslage und Kriegsführung findet auf digitalen Schauplätzen statt und verbindet unkonventionelle Mittel mit nichtstaatlichen Akteuren. Somit verschmelzen die Absichten aus Cyberangriffen und Desinformationskampagnen zum selben Ziel: wirtschaftliche Schäden zu verursachen die zum eigenen ökonomischen Vorteil führen, sowie (demokratie-) politische Institutionen auszuhöhlen indem soziales Misstrauen geschürt wird.[1] Daraus ergibt sich die Wechselwirkung aus Cybersicherheit und Informationssicherheit, welche zwei Seite derselben Medaille darstellen. Daran orientiert sich dieses Impulspapier, welches als Fortführung aus den Jahren 2017 und 2018 zu verstehen ist, und sich folgendermaßen aufgliedert: Zu Beginn wird die Neuentwicklung der Bedrohungslandschaft mit Fokus auf chinesische Cyber-Aggression behandelt, gefolgt von einer Übersicht der Finalisierung der EU-Strategien vis-à-vis Cyber- und Informationssicherheit, welche im Jahr 2018 stattfand. Abschließend werden konkrete Handlungsoptionen und Empfehlungen skizziert, wie hybride Dynamiken vor dem Hintergrund eines globalen Cyber-Rüstungswettlaufs eingedämmt werden können.

2. Evolution der Bedrohungslandschaft

Die europäische Cybersicherheit war 2018 besonders stark von der Debatte um den bevorstehenden Ausbau der fünften Mobilfunkgeneration *5G* geprägt. In diesem Zusammenhang äußerten mehrere Mitgliedsstaaten konkrete Sicherheitsbedenken, allen voran Polen, Deutschland, Frankreich, Dänemark und Tschechien, dass die chinesischen Herstellerkonzerne Huawei und ZTE durch eingebaute Hintertüren Spionageaktivitäten und Cyberangriffe durchführen könnten, was als Gefahr für die nationale Sicherheit eingestuft wurde. Diese Dynamik verstärkt sich durch die Mobilfunkerweiterung, da sie als Grundlage für die Einführung des „Internet

der Dinge“[2] (IoT – Internet of Things) dient. Gemeinsam machen Huawei und ZTE rund 40% der Marktausstattung im europäischen Netzwerk- und Kommunikationssektor aus; auf globaler Ebene liegt die chinesische Marktdurchdringung in der Telekommunikationsausrüstung bei knapp 40%.[3]

Außerhalb der EU kam es auch von Seiten der USA, Kanada, Australien und Neuseeland zu scharfer Kritik und Warnungen gegen Huawei. Die Situation spitzte sich im Jänner 2019 weiter zu, als ein angeblicher chinesischer Huawei-Spion in Polen verhaftet wurde. Daraufhin verlautbarte die polnische Regierung nicht nur das Vorhaben Huawei vom 5G-Ausbau auszuschließen, sondern appellierte auch an die EU und NATO eine starke gemeinsame Position gegen den chinesischen Anbieter einzunehmen. Diese Entwicklungen verdichten sich zunehmend, insbesondere nachdem britische ExpertInnen der EU im Februar 2019 konkrete Beweise für Angriffe auf europäische Hard- und Software vorlegten, die zur chinesischen staatsnahen Hackgruppe Advanced Persistent Threat 10 (APT10) zurückverfolgt wurden. Die Gruppe, welche schon seit längerem von europäischen und US-amerikanischen Behörden untersucht wird, griff insbesondere die Luftfahrtbranche, Bau- und Ingenieurunternehmen, sowie den Telekommunikationssektor und staatliche Einrichtungen in mehr als 12 Ländern mit dem Ziel an, geistiges Eigentum zu stehlen und Wirtschaftsspionage zu betreiben.[4] Mögliche europäische Reaktionen darauf, von Sanktionen bis hin zur Implementierung von gemeinsamen Warnsystemen, sind derzeit in Diskussion.

Ein Meilenstein wurde bereits am 12. März 2019 erreicht, als das Europäische Parlament mittels Verabschiedung der Resolution zur neuen Bedrohungslage durch die Präsenz chinesischer Technologie in Europa, sowohl ein gesteigertes Bewusstsein als auch deutliche Handlungsappelle kommunizierte.[5] Besonders problematisch werden in diesem Zusammenhang die neue chinesischen Gesetzeslage zur Staatssicherheit von 2017 gewertet, die besagt, dass StaatsbürgerInnen sowie chinesische Unternehmen und Organisationen verpflichtet sind mit dem Staat im Sinne einer breit und grenzüberschreitenden Auslegung von nationaler Sicherheit zu kooperieren.[6]

Trotz EU-Ambitionen, den bilateralen Dialog über Cybersicherheit mit China auszubauen[7], tragen Fälle wie die Huawei-Spionagevorwürfe zur Verhärtung der europäischen Wahrnehmung vis-à-vis technologischen Sicherheitsrisiken bei. Verknüpft man jene Entwicklungen mit dem chinesischen Bestreben neue Absatzmärkte zu erobern, um das aktuell niedrigste Wirtschaftswachstum der letzten 28 Jahre zu kompensieren, ergibt sich ein möglicher Zusammenhang aus hybriden Cyberangriffen und innerstaatlichen Wirtschaftsambitionen. In der niederländischen Regierungserklärung zur Lage der Europäischen Union vom Jänner 2019 geht dies hervor. Im Zusammenhang mit der Realität sich verändernden geopolitischen Machtstrukturen, ist von einer protektionistischen, staatlich geführten chinesischen Wirtschaft die Rede, die den europäischen Markt untergräbt und sich nicht an das internationale WTO-Regelwerk binden lässt.[8]

3. Finalisierte Strategie – Unzureichende Umsetzung

Seit der Cyberbereich von institutioneller Ebene der EU sowie einzelner Mitgliedsstaaten als neue und hybride Bedrohung deklariert wurde, kam es zu einer formellen Formalisierung von Strategien der Cyber- und Informationssicherheit. Dies manifestierte sich 2013 durch die Cybersecurity Strategy[9] sowie die Verordnung zum erweiterten Mandat der Europäischen Agentur für Netz- und Informationssicherheit (ENISA)[10]. Die Entwicklung jener Dokumente spitze sich in den vergangenen Jahren zu und kam 2018 zu einer Phase der Finalisierung. Ausgehend von jener veränderten Bedrohungslage leiteten sich zentrale Strategiedokumente aus zwei Schlüsselbereichen ab: Cybersicherheit und Informationssicherheit.

Strategien der Cybersicherheit

In einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur ENISA und zum sogenannten „Cybersecurity Act“, erzielten die Europäischen Institutionen nicht nur eine Weiterentwicklung des Rechtsakts zu Cybersicherheit von 2017, sondern erweiterten auch das Mandat der ENISA. Ein neuer EU-Rahmen zur Cybersicherheitszertifizierung soll so die Sicherheit von Hard- und

Software sowie online Leistungen verstärken, während auf EU-Ebene die Kapazitäten zur Cybersicherheit ausgebaut und gebündelt werden.

Die wichtigsten Hauptmerkmale und Forderungen der Verordnung beinhalten unter anderem:[11]

- Die Einführung von digitalen **Cyber-Sicherheitsstandards,**[12] um die nationale und individuelle Sicherheit sowie die soziale, wirtschaftliche, und politische Stabilität Europas zu gewährleisten. Dazu zählen unter anderem die Definition gemeinsamer Werte, Normen und Verhaltenskodizes sowie ein globaler Ansatz zur Wahrung der Netzwerk- und Informationssicherheit. Die Europäische Union könnte in diesem Zusammenhang eine Vorreiterrolle einnehmen, um eine engere internationale Kooperation im Bereich der Cybersicherheit voranzutreiben.
- Die Förderung der intensiven **Kooperation** und des umfassenden **Informationsaustuschs** zwischen Mitgliedsstaaten und EU-Institutionen zum grenzüberschreitenden Schutz vor Cyberangriffen. Dazu soll die ENISA vermehrt Synergien mit anderen EU-Institutionen errichten, wie unter anderem mit der Computer Emergency Response Team der Europäischen Union (CERT-EU).
- Den Ausbau nationaler **Fähigkeiten,** um sowohl präventiv als auch reaktiv auf Cyberbedrohungen aller Art zu reagieren. Darüber hinaus sollen ebenfalls die **Kapazitäten** und Möglichkeiten auf EU-Ebene ausgebaut werden, um die Mitgliedsstaaten in ergänzender und koordinierender Rolle zu unterstützten. Dies betrifft sowohl menschliche als auch technische Ressourcen.
- Gleichzeitig soll es in weiterer Folge zu einer Effizienzsteigerung im Einsatz gegen Cyberangriffe kommen. Jene Optimierung reicht von der **Vermeidung von Doppelarbeit** durch Koordinierung bis hin zur Entwicklung und Umsetzung von **Best Practices** durch einen transparenten Austausch und offene Kommunikation.
- Die ENISA soll Mitgliedsstaaten bei der Erweiterung und Durchführung von **Trainings- und Bildungsmaßnahmen** im Bereich der Cybersicherheit fördern. Die Errichtung von nationalen Trainingscenter wird in diesem Zusammenhang als wünschenswert erwähnt. Diese könnten außerdem als Verbindungs- und Koordinierungsstellen für einen mitgliedsstaatenübergreifenden Wissenstransfer dienen. Somit würde nicht nur die **Bewusstseinsbildung** innerhalb der Bevölkerung über Themen der Cybersicherheit gestärkt werden, sondern die Europäische Union könnte sich als führendes **Kompetenz- und Exzellenzzentrum** global positionieren.
- Um das fluide Feld der Cybersicherheit auf nachhaltige und ganzheitliche Art und Weise zu behandeln, soll nicht nur eine Momentaufnahme als Analysegrundlage dienen, sondern darüber hinaus müssen auch zukünftige Entwicklungen mitberücksichtigt werden. Das regelmäßige Erstellen von **systematischen Prognosen und innovativen Zukunftsaussichten** soll in diesem Zusammenhang gefördert werden, um sicherzustellen, dass Maßnahmen der Cybersicherheit am Puls der Zeit bleiben, neue Gefahren frühzeitig erkannt und präventiv bekämpft werden können und somit eine langfristige Widerstandsfähigkeit ermöglicht wird.
- Darüber hinaus wird appelliert, dass europäische Akteure auch einen engeren Austausch und eine erweiterte Kooperation mit Institutionen außerhalb der EU-Strukturen forcieren sollten. Im Speziellen die ENISA soll gegebenenfalls eine **intensivierte Koordinierung entlang eines Cybersicherheit-Kooperationsrahmens** mit Organisationen wie der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), der Organisation für europäische wirtschaftliche Zusammenarbeit (OECD) oder der Nordatlantikpakt-Organisation (NATO) andenken. Solche Kooperationsfelder könnten unter anderem gemeinsame Cybersicherheitsübungen oder die Koordinierung eines Vorfallreaktionsplans betreffen.

Ausgehend von jenen ausführlichen und teils bislang unkonventionellen Forderungen nach mehr Handlungsspielraum und einem erweiterten Mandat der ENISA als transeuropäische Dachorganisation der Cybersicherheit, muss hervorgehoben werden, dass die Integrität und Selbstbestimmung der einzelnen EU-Mitgliedsstaaten vollständig erhalten bleibt. Es wird mehrmals ausdrücklich darauf hingewiesen, dass die Verordnung nicht darauf abzielt die

Kompetenzen der Mitgliedsstaaten zu untergraben, sondern zu ergänzen.

Strategien der Informationssicherheit

Im Bereich der Informationssicherheit war 2018 der "Aktionsplan gegen Desinformation"[13] der Europäischen Kommission richtungsweisend, indem sich die Kommission direkt an die Mitgliedsstaaten, das europäische Parlament, den Rat der EU, den Europäischen Rat, den Europäischer Wirtschafts- und Sozialausschuss und den europäischen Ausschuss der Regionen richtete. Der Aktionsplan ist die Antwort auf die Forderung des Europäischen Rates nach Maßnahmen „zum Schutz der demokratischen Systeme der Union und zur Bekämpfung von Desinformation, auch im Kontext der bevorstehenden Wahl zum Europäischen Parlament".[14] In Anbetracht der Wahlen zum Europaparlament im Mai 2019 sowie der über 50 präsidentiellen, nationalen oder lokalen Wahlen in Mitgliedsstaaten der EU bis 2020, ist es von äußerster Wichtigkeit einen sicheren, freien und fairen demokratischen Prozess gewährleisten zu können, welcher resilient gegenüber Desinformationskampagnen ist. Umfragen zufolge sahen sich 80% der EuropäerInnen bereits direkt mit irreführenden oder falschen Onlineinformationen konfrontiert während 83% der europäischen Bevölkerung angibt, dass jene verfälschten Nachrichten eine Gefahr für die Demokratie darstellen.[15] Vor diesem Hintergrund definiert der Aktionsplan Desinformation gleich zu Beginn als nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und eine Bedrohung der öffentlichen Güter und Sicherheit darstellen.

Der Aktionsplan behandelt unter anderem die folgenden Forderungen:[16]

- Die Einführung eines **Verhaltenskodexes** für Social-Media-Plattformen (Facebook, Google, Youtube, Twitter), Software-Anbieter (Mozilla), der Werbebranche und eine Reihe von Berufsverbänden von Online-Plattformen.
- Die Einrichtung und Finanzierung eines Netzwerks aus unabhängigen **FaktenprüferInnen,** welche Desinformationen identifiziert und Fehlinformationen als solche kennzeichnet. Dies stellt die Basis für rigorose technische und politische Untersuchungen sowie Analysen zur **Erleichterung der Rückverfolgung** dar.
- Den Ausbau von **Bildungsinitiativen** sowie bewusstseinsbildende Maßnahmen zur **Förderung der Medienkompetenz** und digitalen Achtsamkeit der europäischen Bevölkerung auf staatlicher und europäischer Ebene entwickelt und umgesetzt werden.
- Die Kategorisierung von Desinformationskampagnen als **Teil einer hybriden Kriegsführung**, welche Cyberangriffe und das Hacken von Netzwerken einschließt. Staatliche Akteure (allen voran Russland) setzten zunehmend Desinformationsstrategien ein, um gesellschaftliche Debatten zu beeinflussen, soziale Spaltungen zu verschärfen und in demokratische Entscheidungsprozesse einzugreifen. Die Bekämpfung jener Absichten setzt ein erweitertes Bewusstsein über dieselben voraus.
- Ein verstärktes **Zusammenarbeiten mit den Ländern der Östlichen Partnerschaft sowie der Südlichen Nachbarschaft** im gemeinsamen und aktiven Kampf gegen manipulative Fehlinformation zur Steigerung der regionalen Resilienz.
- Die Förderung des freien Meinungsaustausches und uneingeschränkten Zugangs zu Medien, zur Stärkung von **unabhängigen Medien und investigativen JournalistInnen**, welche essenziell für das Funktionieren einer demokratischen Gesellschaft sind.
- Die Stärkung der **Rolle der Zivilgesellschaft und der Privatwirtschaft**. Insbesondere Betreiber und Hauptakteure Social-Media-Plattformen sind hierbei gefragt verstärkt Verantwortung über die verbreiteten Inhalte zu übernehmen.

Aus jenen Forderungen kristallisieren sich vier Hauptbereiche heraus:

1. Die Verbesserung der Fähigkeiten der EU-Organe zur Ermittlung, Analyse und Aufdeckung von Desinformation.
2. Die Stärkung koordinierter und gemeinsamer Reaktionen auf Desinformation durch die Einrichtung von Schnellwarnsystemen.

3. Die Mobilisierung des privaten Sektors zur Bekämpfung von Desinformation.
4. Die Sensibilisierung und Verbesserung der gesellschaftlichen Widerstandsfähigkeit.

Strategien innerhalb der EU-Mitgliedsstaaten

Mit Bezug auf die Strategien der einzelnen Mitgliedsstaaten fand eine Analyse über die Unterschiede der nationalstaatlichen Zielsetzungen sowie die Prioritätenlegung im Bereich der Strategien betreffend Cyber- und Informationssicherheit statt. In den herangezogenen Strategiedokumenten betreffend Cybersicherheit können anhand der durchgeführten Untersuchungen folgende Prioritäten der Mitgliedsstaaten dargelegt werden: wirksame Rechtsdurchsetzung, Ausbau von Kapazitäten, Resilienzsteigerung und Bildung und Bewusstseinsförderung.

Aus den staatlichen Papieren geht hervor, dass die Mehrheit der EU-Mitglieder die Zielsetzung auf internationale Kooperationen ausgerichtet ist, zur Etablierung von Krisenbewältigungsmaßnahmen und zum Schutz von kritischer Infrastruktur.[17] Auch die Aufklärung und Bewusstseinsbildung der Zivilbevölkerung ist im Fokus der staatlichen Initiativen. Folglich ergibt sich der Trend, dass sowohl die Rechtsdurchsetzung als auch die Förderung des zivilen Bewusstseins als Prioritäten bevorzugt werden. Die Strategiepapiere zeigen jedoch Mängel in der Entwicklung von Fähigkeiten und Kapazitäten, einschließlich in der Bereitstellung von privatwirtschaftlichen Anreizen zur Verbesserung der digitalen Sicherheit sowie dem Ausbau von öffentlich-privater Zusammenarbeit. Irland, Griechenland und Malta zeigen sich in diesem Zusammenhang am wenigsten engagiert, während Spanien, Finnland, Italien, Estland, Frankreich, Polen und Luxemburg die Vorreiterrollen einnehmen – die restlichen 17 Staaten, einschließlich Österreich, befinden sich auf der Ebene der Cybersicherheitsstrategien im Mittelfeld[18].

Im Bereich der Strategien gegen Desinformationskampagnen, im Speziellen hinsichtlich der politischen Zurkenntnisnahme und Gegenmaßnahmen in Verbindung mit russischen Manipulationsambitionen, gibt es unterschiedliche Herangehensweisen der EU-Staaten. Während die oben genannten wenig engagierten Staaten ebenfalls kaum Engagement in den Strategien der Informationssicherheit zeigen, weisen Schweden, Litauen und Lettland überdurchschnittlich hohe Bereitschaft gegen Fehlinformation vorzugehen auf.[19] Aus der österreichischen Strategie geht hervor, dass weder in der der Gefahrenwahrnehmung noch in der Ausführung von möglichen Gegenmaßnahmen eine klare Linie verfolgt wird. Daher ist sie im Vergleich zu Strategien anderer EU-Staaten unter dem Durchschnitt einzuordnen. Hier besteht akuter österreichischer Handlungsbedarf in der Vertiefung der Strategien, ohne welchen ein zukünftiger Schutz gegen äußere und innere Manipulation und Destabilisierungsambitionen nicht stattfinden kann.

Eine detaillierte Ausfassung der jeweiligen Analyseindikatoren, die zur Erstellung jener Kategorisierung herangezogen wurden, sowie Grafiken zu den einzelnen Teilbereichen, sind auf Nachfrage verfügbar.

4. Conclusio

Die Gefahrenlandschaft aus Cyberunsicherheit und Gefahren der Desinformation ist durch die schnelllebigen technologischen Entwicklungen und die dadurch entstehenden Abhängigkeiten zunehmend komplex und permanent im Wandel. Dies macht jene veränderte Dynamik, mit seinen (teils) neuen Akteuren, immateriellen Mitteln und destabilisierenden Konsequenzen zu einem konstanten sicherheitspolitischen Anliegen von StrategInnen und EntscheidungsträgerInnen.

Die Institutionen der EU und seiner Mitgliedsstaaten sind daher gefordert, die entwickelten Strategien und das vorhandene Bewusstsein in Handlungen umzusetzen. Basierend auf den Analysen und dem Erfahrungsgewinn der letzten Jahre, war 2018 ausschlaggebend für die Formalisierung von strategischen Leitfäden, welche in erste Umsetzungsmaßnahmen mündeten.

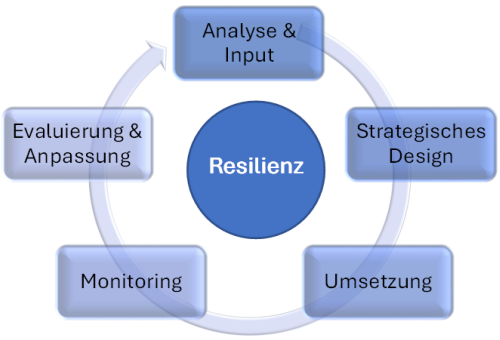

Abbildung 1 – Der „Cyber-Eskalationskreislauf

Jedoch sind jene ersten Handlungen erst der Beginn und nicht das Ende einer umfassenden Resilienzsteigerung gegen hybride Bedrohungen. Bislang kam es weder zu einem Monitoring oder Evaluierungen von Cyberbedrohungen, noch zu den notwendigen (institutionellen) Anpassungen, die zur **konstanten** Weiterentwicklung der Strategien und deren Umsetzung unerlässlich ist. Die Implementierung einer fundierten Verteidigungsstrategie gegen Cyberangriffe und Desinformation ist ein permanentes und allgegenwärtiges Sicherheitsanliegen, auf welches unsere digitalisierte Gesellschaft, Wirtschaft und Politik präventiv und ad hoc reagieren muss. Auf diesen fluiden Permanentzustand des Cyber-Eskalationskreislaufs muss daher ein ebenso permanenter Kreislauf aus sich stets neu erschaffenden Gegenmaßnahmen und institutioneller Weiterentwicklung zur Wahrung der inneren Sicherheit und Stabilität folgen.

About the Author

Michael Zinkanell, M.A./B.A., ist Research Fellow am Austria Institut für Europa- und Sicherheitspolitik (AIES). Neben seiner Expertise in europäischer Sicherheits- und Verteidigungspolitik sowie geopolitischen Entwicklungen liegt sein analytischer Schwerpunkt auf der Analyse der sicherheitspolitischen Implikationen von hybriden Bedrohungen, Desinformationskampagnen und Cyberattacken.

[1] EEAS, *„A Europe that Protects: Countering Hybrid Threats"*, 16 June 2018. Download: https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en

[2] Ist der Zustand der exzessiven digitalen Vernetzung von physischen Maschinen und virtuellen Programmen. Die Automatisierung technischer Geräte (von kommerziellen Haushaltsgegenständen bis hin zu komplexen industriellen Maschinen) wird durch die direkte Verbindung und Kommunikation jener vorangetrieben. Das IoT wird von ExpertInnen als das Rückgrat der globalen Konnektivität bezeichnet.

[3] Dell'Oro Group, *„THE TELECOM EQUIPMENT MARKET 3Q 2018"*, 2018. Download: http://www.delloro.com/delloro-group/key-takeaways-telecom-equipment-market-3q-2018

[4] Bloomberg, *„EU Considers Response to China Hacking After U.K. Evidence, Sources Say"*, 11.02.2019. Download: https://www.bloomberg.com/news/articles/2019-02-11/eu-is-said-to-mull-response-to-china-hacking-after-u-k-evidence

[5] European Parliament Press Release, *„MEPs adopt Cybersecurity Act and want EU to counter IT threat from China"*, 12.03.2019. Download: http://www.europarl.europa.eu/news/en/press-room/20190307IPR30694/meps-adopt-cybersecurity-act-and-want-eu-to-counter-it-threat-from-china

[6] European Parliament, "*Joint Motion for a Resolution on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP))"*, 08.03.2019, Download: http://www.europarl.europa.eu/doceo/document/RC-8-2019-0154_EN.pdf

[7] Im September 2017 fanden erstmals Gespräche zu Cybersicherheit mit China und anderen Staaten wie Südkorea, Indien, Japan und den USA statt.

[8] Dutch Ministry of Foreign Affairs, "*State of the European Union 2019 Letter to the President of the House of Representatives on the State of the European Union 2019"*, 2019. Download: https://www.government.nl/documents/parliamentary-documents/2019/02/04/state-of-the-european-union-2019

[9] European Commission, "*JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*", 07.02.2013. Download: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[10] European Parliament and Council of the European Union, "*REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.*", 21.05.2013. Download: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0526&from=DE

[11] Council of the European Union, „*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "European Union Agency for Cybersecurity", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*", 20 December 2018. Download: https://www.parlament.gv.at/PAKT/EU/XXVI/EU/04/86/EU_48658/imfname_10868281.pdf

[12] Die erste EU-weite Cybersicherheitszertifizierung wurde durch die Verabschiedung des Cybersecurity Acts vom 12.03.2019 eingeführt. Siehe: http://www.europarl.europa.eu/news/en/press-room/20190307IPR30694/meps-adopt-cybersecurity-act-and-want-eu-to-counter-it-threat-from-china

[13] European Commission: *„Action Plan against Disinformation"*, 05.12.2018. Download: https://cdn1-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/lpM1X9RnuE28GrR78F7yFA0HtKjii4TzKMvXoSg5Bn0/mtime:1544008849/sites/eeas/files/action_plan_against_disinformation.pdf

[14] Schlussfolgerungen des Europäischen Rates vom 18. Oktober 2018.

[15] European Commission, *„Flash Eurobarometer 464"*, February 2018. Download: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/%20surveyky/%202183

[16] European Commission: *„Action Plan against Disinformation"*, 05.12.2018. Download: https://cdn1-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/lpM1X9RnuE28GrR78F7yFA0HtKjii4TzKMvXoSg5Bn0/mtime:1544008849/sites/eeas/files/action_plan_against_disinformation.pdf

[17] ENISA, "*National Cyber Security Strategies (NCSSs) Map*". Link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[18] ENISA, "*National Cyber Security Strategies (NCSSs) Map*". Link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[19] European Values, "2018 Ranking of countermeasures by the EU28 to the Kremlin's subversion operations", 15.08.2018. Download: https://www.kremlinwatch.eu/userfiles/2018-ranking-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations.pdf