IFSH
Institute for Peace Research
and Security Policy
at the University of Hamburg

IFAR²
Interdisziplinäre Forschungsgruppe
Abrüstung
Rüstungskontrolle und
Risikotechnologien

IFAR² Fact Sheet

Cyber Space, Cyber Attack and Cyber Weapons

A Contribution to the Terminology

Nick Ebner *October 2015*

The term *cyber space* has attracted enormous attention over the last few years. People are becoming more and more dependent on digital technologies. *Cyber space* touches almost everything and everyone. From this dependency, it follows that attacks targeted on or through *cyber space* might have severe effects on a society: cyber-attacks on critical infrastructures such as the energy supply, communication systems, financial markets or the military infrastructure, have a great destructive potential. As a result, cyber security today is almost omnipresent in national and international security politics. In a recent report about IT-security, German Interior Minister, Thomas de Maizière, warned of the high potential for IT-security endangerment in Germany[1]. Further, since 2009, the Obama administration, in its security strategy, has strongly focused on cyber security. According to the White House, cyber security is seen as "one of the most serious economic and national security challenges"[2]. *Cyber space is*, however, not only a challenge for national security, but also offers new means of waging war. In fact, in the meantime, *cyber space* is widely seen as the fifth domain of warfare by, the military. The U.S. Department of Defense, for example, states that "although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space"[3]. In addition, its technical and man-made origin, *cyber space,* just like *cyber-attack,* has lately expanded to become an abstract political term used in many different ways.

This paper focuses on the political use of the terms *cyber space, cyber-attacks, as well as cyber weapon*. More precisely, it aims at sketching a picture of current international disputes related to threats in *cyber space*. Therefore, it first needs to be clarified what international actors mean by *cyber space*. Second, threats in *cyber space* are often referred to as *cyber-attacks*. Thus, how *cyber-attacks* are defined by international actors and what they include need to be examined. Third, the use of the term *cyber weapon* needs to be examined in order to cover the major means used for a *cyber-attack*. Thus, this fact sheet offers a summary of different definitions of these essential terms, drawn up by important international actors with the purpose

[1] Bundesamt für Sicherheit und Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014, November 2014, available on: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/bsi-lagebericht-it-sicherheit.pdf?__blob=publicationFile (p.4).

[2] The White House: The comprehensive national cybersecurity initiative, available on: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[3] Lynn, William J., Department of Defense, Defending a New Domain: The Pentagon´s Cyberstrategy, 2010, available on: http://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx

of outlining similarities and differences. Thereby, major disputes as well as some agreement on certain aspects of the matter, can be highlighted.

Cyber Space – a man-made sphere?

While *cyber space* is taking on increasing importance for governmental security strategies, there is still no generally accepted definition of the term *cyber space*. The four definitions below were chosen to offer a variety of definitions from different actors: Germany was selected due to its major role and central geographical position in the EU. The USA is one of the major players in the world and its support will be necessary for an internationally accepted definition. The International Telecommunication Union (ITU) is a specialized agency of the United Nations that is skilled in information and communication technologies. The Tallinn Manual on the International Law Applicable to Cyber Warfare (henceforth: Tallinn Manual) adds a legal and a non-governmental perspective. The Tallinn Manual is an academic study on how international law applies to cyber conflicts, written by an international group of law experts. Therefore, on the one hand, the actors selected reflect governmental approaches to cyber space and, on the other hand, legal and technological expertise on *cyber space* are provided.

Germany defines *cyber space* as "*the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace".*[4]

The **USA** holds that it is „ *a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".*[5]

The **International Telecommunication Union** (ITU) uses the term cyber environment. "*This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks."* [6]

Finally, in the **Tallinn Manual**, *cyber space* is described as "*the environment formed by physical and non-physical components, characterized by the use of computers and electromagnetic spectrum, to store, modify and exchange data using computer networks*".[7]

In addition to the four definitions above, 21 additional definitions by different actors were taken into account for the analysis in order to identify overlaps and significant differences (see table 1).[8]

It should be mentioned first of all that all actors conceptualize *cyber space* within different levels (see Table 2): The first is the virtual level which includes software and bytes. All 25 actors mention the virtual level in their definitions. The second is the physical level that includes hardware and infrastructure. Twelve actors, including the USA and the Tallinn Manual, mention the physical level. This can be seen as a major dispute: While twelve actors include infrastructure in their definitions,

[4] Federal Ministry of the Interior: Cyber Security Strategy for Germany, February 2011, available on: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=5B6636607CB58EFBB61431566F7E5B15.2_cid334?__blob=publicationFile (p.14).

[5] Department of Defense: Dictionary of Military Terms, available on: http://www.dtic.mil/doctrine/dod_dictionary/.

[6] International Telecommunication Union: Series X: Data networks, open system communications and security: overview of cybersecurity, 2008, available on: http://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=en&rlink={3E2AC1A2-9D18-4235-80B6-7946B3266788}.

[7] Michael N. Schmidt (editor): Tallinn Manual on the International Law applicable to cyber warfare, Cambridge University Press, New York, available on: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=0/1803379#search (p.278).

[8] See appendix for further definitions.

there are thirteen actors which exclude infrastructure from their definitions (Germany and the ITU for example). Furthermore, the ITU and the USA, as well as ten other actors, add the "human domain" as a third level by stating that *cyber space* includes the human individuals and users of cyber space, too.[9]

The interconnection or interdependence of networks or IT systems is another congruent component of the twenty definitions. With the exception of the Tallinn Manual, all the definitions above include the interconnection of networks. In addition, thirteen actors (the USA among others) note that this interconnection is global.

In a nutshell, there is general agreement that *cyber space* includes a virtual level of interconnected and interdependent networks. Some hold that *cyber space* has a physical level and a human domain, too.

Cyber Attack – a politicized term?

The definition of *cyber-attack* is crucial to the question of how to deal with *such an attack* and that is why it is highly disputed. In the following, there is an outline of the major issues around *cyber-attacks*: The response to an attack via *cyber space* is, first of all, going to differ depending on the identified perpetrator (state or non-state actor, see Figure 1). While non-state actors must face prosecution, an attack by a state actor can either be in the context of an armed conflict or in the context of peace. If the *cyber-attack* is executed in times of an armed conflict, the major question is the applicability of International Humanitarian Law. In times of peace, the kind of attack (cybercrime, cyber espionage or cyber sabotage) and its level of impact (e.g. access, manipulation, disruption, damage or destruction) are going to be essential for this question if the attack can be seen as a use of force. If so, the state attacked may use its right to self-defense according to international law.

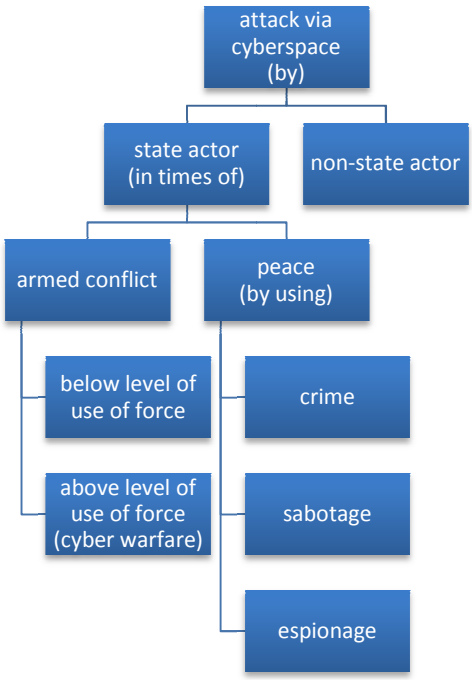

Figure 1: Options for cyber attacks

With this in mind, there is an obvious need for an internationally accepted definition for *cyber-attack*. So far, however, the international actors have not been able to reach an agreement. In fact, the definitions of *cyber-attack* by different actors vary strongly. In the following, there is a selection of definitions that might offer different approaches to *cyber-attacks*: Next to Germany and the USA, NATO is taken into account as it might be interesting to examine a military alliance and its approach to *cyber-attacks*. Again, the Tallinn Manual adds a legal and non-governmental perspective.

Germany defines a *cyber-attack* as *"an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability, may all or individually be compromised. Cyber-attacks directed against the confidentiality of an IT system, which are launched or managed by*

[9] Alwardt, Christian/Neuneck, Götz: Kurz- und mittelfristige technologische Bedrohungen und Risiken, p.52, in: Analyse sicherheitspolitischer Bedrohungen und Risiken unter Aspekten der Zivilen Verteidigung und des Zivilschutzes, Ehrhart, Hans-Georg/Neuneck, Götz (eds.), p.23-79, Nomos, Baden-Baden, 2015.

foreign intelligence services, are called cyber espionage. Cyber-attacks against the integrity and availability of IT systems are termed cyber sabotage".[10]

The **USA** holds that a *cyber-attack* can be defined as "*a hostile act using computer or related networks or systems, and intended to disrupt and/ or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves – for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.*[11]"

NATO uses the term computer network attack and defines it as an "*action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself".*[12]

Finally, the **Tallinn Manual** states more broadly that *"a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.*[13]"

Figure 2 highlights that there are many more differences than overlaps between the definitions of the four actors. However, there is one major agreement in the definitions by Germany, USA, NATO and, to some extent, in the Tallinn Manual, and that is the inclusion of cyber sabotage. Therefore, an attack targeted at the integrity and/or availability of IT systems constitutes a *cyber-attack* according to Germany, the USA and NATO. Apart from this, the definitions above vary in some essential questions as can be seen in the following paragraph.

1. *Does an attack executed by a non-state actor qualify as a cyber-attack?*

   There is broad agreement that non-state actors can trigger a cyber threat. However, non-state actors are not explicitly named as possible actors of a *cyber-attack*

CYBER ATTACK	Germany	USA	NATO	Tallinn Manual
Attacker	Cyber espionage: launched/managed by foreign intelligence service → only state actors Cyber sabotage: unspecified	Unspecified	Unspecified	Predominantly state actors
Context	Peace (and armed conflicts)	Peace (and armed conflicts)	Peace (and armed conflicts)	Armed conflicts
Type of attacks	Cyber espionage and cyber sabotage	cyber sabotage	cyber sabotage	Cyber-attacks in armed conflicts
Level of impact	Confidentiality, integrity and/or availability	Integrity and/or availability	Integrity and/or availability	Injury or death to persons or damage or destruction to object

Figure 2: Four definitions for cyber attacks and their specifics

[10] Federal Ministry of the Interior: Cyber Security Strategy for Germany, February 2011, available on: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=5B6636607CB58EFBB61431566F7E5B15.2_cid334?__blob=publicationFile (p.14).

[11] Department of Defense: Cyberspace Operations Lexicon, available on: https://info.publicintelligence.net/DoD-JointCyberTerms.pdf (p.5).

[12] NATO glossary of terms and definitions, 2014, available on: http://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF (2-C-11).

[13] Michael N. Schmidt (editor): Tallinn Manual on the International Law applicable to cyber warfare, Cambridge University Press, New York, available on: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=0/1803379#search (p.106).

in any of the definitions above. Rather, explicit references to the person(s) or organization(s) responsible are avoided (e.g. USA or NATO). **Germany** is a little more explicit, stating that acts of cyber espionage are limited to those executed by state actors.

The **Tallinn Manual** is restricted to *cyber-attacks* in the context of armed conflicts. According to the Tallinn Manual, a *cyber-attack* "constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".[14] Thus, *cyber-attacks* are predominantly executed by state actors. However, an attack by a non-governmental organization, provided with the requirements for the attack by a state, qualifies as a *cyber-attack* as well, according to the Tallinn Manual.[15]

2. *Does an attack targeted at confidentiality qualify as a cyber-attack? Is cyber espionage a cyber-attack or a cybercrime?*

   A much disputed question is whether an attack on the confidentiality of an IT system, that constitutes cyber espionage, is a *cyber- attack* or not. Some argue that cyber espionage is first of all a cybercrime and needs to be prosecuted as a "theft of commercial intellectual property and proprietary information, of data with significant economic value, or the theft of government sensitive and classified information".[16] The dividing line between cybercrime and cyber espionage is vague. As most acts of cyber espionage do not qualify as an attack under international law, the majority of actors exclude cyber espionage from their definitions (e.g. USA, NATO). **Germany** is an exception by taking into account acts of cyber espionage executed by state actors.

   The **Tallinn Manual**, by contrast, does not ask this question since, for the Tallinn Manual, the severity of the effects of a *cyber-attack,* not the means used, are crucial. For the same reason, cyber sabotage, just like cyber espionage, does not necessarily qualify as a *cyber-attack* according to the Tallinn Manual, since the act of cyber sabotage needs to reach the level of use of force to qualify as *cyber-attack*.

3. *In case of an attack in cyber space, what level of impact must there be in order to qualify as cyber-attack? Is a cyber-attack a use of force?*

   For **Germany**, an attack causing damage or compromise of "confidentiality, integrity and/or availability" of IT-Security qualifies as a *cyber-attack*. The **USA**, by focusing on sabotage, has a narrower definition: A *cyber-attack* involves the disruption and destruction of "critical cyber systems, assets, or functions". **NATO** follows a similar logic and mentions the disruption, denial, degrading or destruction of information and/or computer and/or computer network. None of them puts a *cyber-attack* on a par with the use of force. The severity of a *cyber-attack* is going to be decisive if it reaches the level of a use of force according to international law.

   According to the **Tallinn Manual**, one can refer to a *cyber-attack* if it causes "*injury or death to persons or damage or destruction to objects"*. A *cyber-attack* is, therefore, inevitably a use of force according to the authors.

[14] Ibid. (45)
[15] Ibid. (46)
[16] Klimburg, Alexander: National Cyber Security Framework Manual, CCDCOE, 2012: p.16.

CYBER ATTACK	Executed in times of peace	Executed in armed conflicts
Actors	Mainly by state actors	Mainly by state actors
Legal issue	Application of *jus ad bellum*	Application of *jus in bello*
Main dispute	(When) does a *cyber-attack* justify a use of force so that the right of self-defense applies for the attacked state?	(When) does a *cyber-attack* reach the level of a use of force so that IHL applies?
Viewpoints in research	Consensus that a categorization of the effects of *cyber-attacks* is needed, and that internationally accepted definitions for the terms *cyber-attack, cyber space and cyber weapon* are also needed	2 different approaches: permissive (allowing a wide range of *cyber-attacks* against the civilian population) vs. restrictive approach (restricting *cyber-attacks* as a matter of law)[17]
Legal papers	Charter of the United Nations	Tallinn Manual, IHL (Additional Protocol I of the Geneva Convention of 1949)

Figure 3. Cyber-attacks in peace and armed conflict in legal studies

Cyber Weapon – a non-bulletproof term:

Disruptive *cyber means*, as seen before, can be used for a wide range of purposes: crimes, espionage, and sabotage, as a means of threat, as self-defense or as a means in war. The distinction between *cyber weapons* and other, non-violent cyber means is vague but essential: First, for a possible political or military response by a state, it makes a difference whether a cyber means has the potential to harm persons or objects.[18] Second, a classification is necessary for possible arms control initiatives.[19] Consequently, as always, a generally accepted definition is an important first step.

Only few actors have, so far, defined the term *cyber weapon* and there is, again, no consensus. In this paper, the definitions mentioned in an OECD study, of Russia and of the Tallinn Manual are taken into account. Russia and the OECD members represent major actors on the international stage. The OECD study is part of an OECD project and does not necessarily reflect the official view of the OECD. The Tallinn Manual, as stated before, offers a non-governmental and legal perspective. (See Figure 3)

According to the **OECD study** *"cyberweapons include: unauthorised access to systems ("hacking"), viruses, worms, trojans, denial of service, distributed denial of service using botnets, root-kits and the use of social engineering. Outcomes can include: compromise of confidentiality / theft of secrets, identity theft, web-defacements, extortion, system hijacking and service blockading. Cyberweapons are used individually, in combination and also blended simultaneously with conventional "kinetic" weapons as force multipliers".*[20]

Russia uses the term information weapon and defines it as "*information technology, tools, and methods used for the purpose of information warfare".*[21]

The **Tallinn Manual** states that *"Cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of cyber operation as an attack (Rule 30). […] Cyber means of warfare include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed,*

[17] Michael. N. Schmidt: Rewired warfare: rethinking the law of cyber-attack; in: International Review of the Red Cross, 2014, 96, p.191.
[18] Rid, Thomas/McBurney, Peter: Cyber-Weapons, RUSI Journal, 157, 2012, p.11.
[19] Ibid.

[20] Sommer, Peter/Brown, Ian: Reducing Systemic Cybersecurity Risk, January 2011, available on: http://www.oecd.org/gov/risk/46889922.pdf (p.6).
[21] NATO CCD COE: Conceptual views regarding the activities of the armed forces of the Russian Federation in the information space, unofficial translation, available on: https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf (p.5).

or intended to be used to conduct a cyber-attack (Rule 30)".[22]

CYBER WEAPON	OECD study	Russia	Tallinn Manual
Context	Armed conflict	Armed conflict	Armed conflict
Coverage of definition	Specific list of *cyber weapons,* still broad coverage: *"unauthorised access to systems ("hacking"), viruses, worms, trojans, denial of service, distributed denial of service using botnets, root-kits and the use of social engineering"*	Broad coverage: *"information technology, tools, and methods"*	Broad coverage: *"any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber-attack"*
Threshold cyber means/ cyber weapons	Any cyber means supporting warfare are *cyber weapons*	Any cyber means supporting warfare are *cyber weapons*	Any cyber means used for a cyber-attack are *cyber weapons*

Figure 4: Comparison of different definitions on cyber weapons

The focus on armed conflicts by the **OECD and Russia** confirms the political uncertainty about how to classify cyber means in times of peace. Most states, like the USA, avoid defining *cyber weapons* at all, stating that it is "difficult".[23] Plus, it seems to be easier to define *cyber weapons* in the context of an armed conflict (e.g. OECD, Russia), because it avoids some pitfalls: In times of peace, it makes a huge difference whether a cyber mean used against a nation can cause harm or not. Consequently, a definition of cyber weapon in the context of peace would have major implications for a nation´s defensive and offensive use of cyber means. In an armed conflict, the key issue is rather whether the use of a cyber means qualifies as use of force. However, the OECD study and Russia do not imply with their definitions that each use of a *cyber weapon* qualifies as a use of force. Therefore, the definitions are innocuous and thus of relatively low value. Again, the definition in the **Tallinn Manual** offers an initial approximation and a good basis for discussing the use of *cyber weapons* in armed conflicts.

Conclusion:

The danger of threats in or through *cyber space* is very present in current international politics, but there is little agreement on how to define central terms. The biggest and most essential controversy is probably the definition of the term *cyber-attack*. Disagreements on defining *cyber space* and *cyber weapon* could probably be solved with an internationally accepted definition of *cyber-attack*. Here, the Tallinn Manual might offer a useful approach and guidance for the context of an armed conflict. For future challenges to prevent the use of disruptive cyber weapons, a great joint effort is needed to achieve a compromise for an applicable acceptance of a definition in the international realm.

[22] Michael N. Schmidt (editor): Tallinn Manual on the International Law applicable to cyber warfare, Cambridge University Press, New York, available on: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=0/1803379#search (p.141f).

[23] Department of Defense Cyberspace Policy Report, November 2011, available on: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf (p.8).

Appendix:

1. Cyber Space Definitions:

Country	Definition	Source
Austria	"Cyber space is the virtual space of all IT systems interconnected at data level on a global scale. The basis for cyber space is the Internet as a universal and publicly accessible connection and transport network, which may be supplemented and expanded through other data networks. In common parlance, cyber space also refers to the global network of different independent IC infrastructures, telecommunication networks and computer systems. In the social sphere the use of this global network allows individuals to interact, exchange ideas, disseminate information, give social support, engage in business, control action, create art and media works, play games, participate in political discussions and a lot more. Cyber space has become an umbrella term for all things related to the Internet and for different Internet cultures. Many countries regard networked ICT and independent networks operating through this medium as components of their "national critical infrastructures"."	https://www.bka.gv.at/DocView.axd?CobId=50999 (p.21)
Belgium	"The global environment that is created through the interconnection of communication and information systems. The cyberspace includes the physical and virtual computer networks, computer systems, digital media and data."	https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf (p.18)
Canada	"Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship."	http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (p.2)
Czech Republic	"Cyber space means digital environment, enabling to create, process and exchange information, created by information systems and services and electronic communication networks."	www.govcert.cz/download/nodeid-1246/ (p.2)
Finland	"Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures. Note 1: Representative to the environment is the utilisation of electronics and the electromagnetic spectrum for the purpose of storing, processing and transferring data and information via telecommunications networks. Note 2: Information (data) processing means collecting, saving, organising, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions on information (data)."	www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy (p.12)
France	"The communication space created by the worldwide interconnection of automated digital data processing equipment."	http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (p.21)
Germany	"Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.	http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=5B6636607CB58EFBB61431566F7E5B15.2_cid334?__blob=publicationFile (p.16)
Hungary	"Cyberspace means the combined phenomenon of globally interconnected, decentralised and ever-growing electronic information systems as well as the societal and economic processes appearing in and through these systems in the form of data and information."	www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx (p.3)
India	„Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks."	http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf (p.1)
International Organization for Standardization (IOS)	"The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."	http://www.iso27001security.com/html/27032.html
International Telecommunication Union (ITU)	Cyber environment: "This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks."	http://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=en&link={3E2AC1A2-9D18-4235-80B6-7946B3266788}
Japan	"Global virtual spaces such as the internet composed of information systems, information communications networks and similar systems and which circulate large quantities of a large variety	http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-

	of information."	en.pdf (p.5)
Kenya	"The notional environment in which communication over computer networks occurs."	http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf (p.12)
Latvia	„Cyber space is an interactive environment that includes users, networks, computing technology, software, processes, information in transit or storage, applications, services, and systems that can be connected directly or indirectly to the Internet, telecommunications and computer networks. Cyber space has no physical boarders."	https://ccdcoe.org/sites/default/files/strategy/LVA_CSS_2014-2018.pdf (p.19f)
New Zealand	"The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place."	http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf (p.12)
Qatar	"A virtual or electronic environment that results from the interdependent network of information and communications technology (e.g., the Internet, telecommunications networks, computer systems, and embedded processors and controllers) that links people with services and information."	http://www.ictqatar.qa/en/documents/document/national-cyber-security-strategy (p.23)
Saudi-Arabia	"A global domain within the information environment consisting of the interdependent networks of information systems infrastructures including the internet, telecommunications networks, computer systems, embedded processors and controllers."	http://www.mcit.gov.sa/Ar/MediaCenter/PubReqDocuments/NISS_Draft_7_EN.pdf (A-2)
South-Africa	"Cyberspace means a physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users.	http://www.cyanre.co.za/national-cybersecurity-policy.pdf (p.6)
Spain	"Cyber space is the set of means and procedures based on Information and Communications Technology which is configured for the provision of services. Cyber space consists of hardware, software, the Internet, information services and systems of control that ensure the provision of services that are essential for the socio-economic activity of any nation, especially those that are connected to its critical infrastructure."	https://www.ismsforum.es/ficheros/descargas/a-national-cyber-security-strategy-.pdf (p.12)
Tallinn Manual	"The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks."	http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=0/1803379#search (p.278)
The Netherlands	"For the purposes of this strategy, "cyberspace" is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc.) present in this domain."	https://ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf (p.4)
Turkey	"The environment which consists of information systems that span across the world including the networks that interconnect these systems. National cyber space: The environment which consists of the information systems that belong to public organizations, natural and legal persons."	https://ccdcoe.org/strategies/TUR_CyberSecurity.pdf (p.8)
Trinidad and Tobago	"Cyberspace integrates a number of capabilities, such as sensors, signals, connections, transmissions, processors, and controllers, and generates a virtual interactive experience accessed for the purpose of communication and control regardless of a geographic location. Cyberspace allows the interdependent network of information technology infrastructures, telecommunications networks, such as the Internet, computer systems, integrated sensors, system control 27 networks and embedded processors and controllers common to global control and communications."	http://www.nationalsecurity.gov.tt/Portals/0/Pdf%20Files/National_Cyber_Security%20Strategy_Final.pdf (p.26f)
UK	"An interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet but also other information systems that support our businesses, infrastructure and services."	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (p.11)
USA	National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.	Cyberspace Policy Review 2009
USA: Department of Defense (DoD)	"A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."	Department of Defense Dictionary of Military and Associated Terms
USA: National Initiative for Cybersecurity	"The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."	National Initiative for Cybersecurity Careers and Studies - A Glossary of Common Cybersecurity Terminology
USA: Committee on National Security Systems (CNSS)	"A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."	CNSS Instruction No. 4009 - 26 Apr 2010

Table 1

2. Cyber Space Graph:

	Virtual level	Physical level	Human level	interdependence/ interconnection	global	inclusion infra-structure	exclusion infra- struc-ture
Austria	I	I	I	I	I	I	
Belgium	I	I		I	I	I	
Canada	I	I	I	I	I	I	
Czech Republic	I	I		I		I	
Finland	I	I		I		I	
France	I			I	I		I
Germany	I			I	I		I
Hungary	I		I		I		I
India	I		I	I	I		I
IOS	I		I				I
ITU	I		I	I			I
Japan	I			I	I		I
Kenya	I						I
Latvia	I		I	I			I
New Zealand	I	I		I	I	I	
Qatar	I		I	I			I
Saudi Arabia	I	I	I	I	I	I	
South Africa	I	I	I			I	
Spain	I	I				I	
Tallinn Manual	I	I				I	
The Netherlands	I			I			I
Turkey	I			I	I		I
Trinidad & Tobago	I	I	I	I	I	I	
UK	I			I			I
USA	I	I	I	I	I	I	
TOTAL	25	12	12	20	13	12	13

Table 2

IFSH, October 2015

Die Interdisziplinäre Forschungsgruppe Abrüstung, Rüstungskontrolle und Risikotechnologien (IFAR²) beschäftigt sich mit dem komplexen Zusammenspiel von rüstungsdynamischen Faktoren, dem potenziellen Waffeneinsatz, der Strategiedebatte sowie den Möglichkeiten von Rüstungskontrolle, Non-Proliferation und Abrüstung als sicherheitspolitische Instrumente. Weitere Informationen unter http://www.ifsh.de/IFAR.

Kontakt:
Christian Alwardt Email: alwardt@ifsh.de Tel. +49 (0)40 866077 - 77
Götz Neuneck Email: neuneck@ifsh.de Tel. +49 (0)40 866077 - 21