REPORT | October 2014

TIM MAURER & ROBERT MORGUS

# Compilation of Existing Cybersecurity and Information Security Related Definitions

**Funding provided by**

Federal Department of Foreign Affairs, Switzerland

*The contents of this report are the sole responsibility of New America and do not necessarily reflect the views of the Swiss Federal Department of Foreign Affairs.*

## About the Authors

Tim Maurer is a Research Fellow at New America focusing on cyberspace and international affairs. His current research examines the global cybersecurity norms process, transatlantic cooperation on security and freedom in the digital age, and swing states in the international Internet governance debate. He is part of New America's Future of War project and the Research Advisory Network of the Global Commission on Internet Governance. In October 2013 and February 2014, he spoke about cyber-security at the United Nations and his research has been published by Harvard University, Foreign Policy, CNN, and Slate among others. He holds a Master in Public Policy concentrating on international and global affairs from the Harvard Kennedy School.

Robert Morgus is a Research Associate at New America where he provides research and writing support on cyberspace and international affairs. His work focuses on swing states in the Internet governance debate, Internet freedom in the context of U.S. export controls, technological sovereignty, and cybersecurity. Robert received his B.A. with honors in diplomacy and world affairs from Occidental College in Los Angeles in 2013.

*We owe special thanks to Martin Sigalow and Scott Janz for providing outstanding research assistance for this project during their time at New America as well as to the people at various institutions who offered valuable resources and feedback.

## Table of Contents

# INTRODUCTION

The year 2013 saw a number of positive developments in regional and global cybersecurity discussions including the Initial Set of OSCE Confidence-Building Measures (CBMs) to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies[1] of the Organization for Security and Co-operation in Europe (OSCE). At the same time, this policy debate continues to face the significant challenge that the Internet Society describes as follows, "as a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and 'solutions' ranging from the technical to the legislative," highlighting the need for a better understanding of what is meant by cybersecurity.[2]

One of the OSCE Confidence-Building Measures, CBM number nine out of eleven, addresses this problem and states:

> "In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavor to produce a consensus glossary."

The goal of this study is to contribute to greater clarity and a understanding regarding terminology related to cyberspace and cybersecurity by offering a collection of existing definitions of related terms primarily provided by international organizations or standard setting bodies as well as by states through national (cyber-) security strategies and documents. These are complemented by terms from a few selected other sources such as the Oxford Dictionary on Computing.

## Methodology

The research process was divided into five phases including several feedback loops: (1) develop list of relevant terminologies, (2) collect and analyze terms published by regional and international intergovernmental organizations and international standard setting bodies, (3) collect and analyze terms used by states in national (cyber-) security strategies and documents, (4) collect and analyze terms outlined in other selected sources, (5) write draft report.

The list of relevant terminologies is outlined in the Table of Contents. Generally, this report should be viewed as a "living document" providing a comprehensive, global collection of existing cybersecurity related terms but certain terms or documents might not be included and we invite the reader to submit any additional terms or documents to the authors. Terms marked with "*" in the Table of Contents are terms that were not initially identified but emerged during the iterative research process as being used in similar contexts and therefore added to this study. These terms were not necessarily part of the search process for all documents and might therefore exist in other documents not listed in this report. Additional definitions for terms that make up the definitions listed in this document, for example, the term "availability," exist, but were outside the scope of this study. This compilation is therefore open to further contributions and will be published together with a new website that will allow practitioners and others to search for specific terms or sources, to submit additional definitions or new documents, and to access the data underlying the report.

---

[1] Organization for Security and Co-operation in Europe, Permanent Council, "Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," *OSCE Plenary*, 2013. <http://www.osce.org/pc/109168?download=true>

[2] Internet Society, "Some Perspectives on Cybersecurity: 2012," *Internet Society,* 2012. <http://www.internetsociety.org/doc/someperspectives-cybersecurity-2012 >

The terms are grouped into thematic buckets starting with more general ones such as "information" and "cyberspace" followed by general security terms such as "cyber security" and "incident" related terms blending over into those with a component relating to intent or type of actor complemented with a list of other terms that did not fit into one or multiple buckets. Within the broader categories, the terms are sorted alphabetically. There are different options to structure such a list and we hope that the reader will find our approach relatively easy to follow and offering a nuanced picture of the breadth and depth of the various terms.

Within each bucket, the various definitions found for each term are organized by their source and in the order outlined below. We start with the five permanent members of the UN Security Council (P5) given their special status under the UN Charter. States that are members of the new (fourth) UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE4)[3] follow given the UNGGE4's important role in this policy area. Given the OSCE's agreement regarding CBMs in December 2013, states that are a member to the OSCE are listed subsequently. Finally, terms used by any other state are included in this document. Terms outlined in documents by intergovernmental organizations are organized alphabetically by the name of the intergovernmental organization. The same logic applies to other sources.

- State
    - A state who is a P5
    - A state who is not a P5 but member of the UNGGE4
    - A state who is neither a P5 nor a UNGGE4 member but a member state of the OSCE
    - A state who is neither a P5, UNGGE4 nor OSCE member
- Intergovernmental Organization
    - African Union
    - Commonwealth of Independent States
    - Council of Europe
    - Economic Community of West African States
    - European Union
    - International Telecommunication Union
    - League of Arab States
    - North Atlantic Treaty Organization
    - Organization for Economic Cooperation and Development
    - Organization for Security and Cooperation in Europe
    - Shanghai Cooperation Organization
- Other Source
    - EastWest Institute and Institute for Information Security Issues of Moscow State University (EWI/IISI)
    - Institute of Electrical and Electronic Engineers
    - International Organization for Standardization
    - Internet Engineering Task Force
    - Internet Society
    - Oxford Dictionary of Computing (2004 & 2008)
    - Oxford English Dictionary

[3] Belarus, Brazil, China, Colombia, Egypt, Estionia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russia, South Korea, Spain, United Kingdom, and United States participate in the UNGGE4.

Definitions come in many different forms. Some are explicitly listed in a dictionary or glossary. Others are part of a longer text but explicitly state that term A means X, Y, and Z. At times, full or partial passages do not clearly state a definition, but the context in which a term is being used offers a meaning to the reader. The terms listed in this study are coded based on where in the text of a document the definition was found. Some definitions are in a foreign language and for some of them the authors provided unofficial translations. The authors also invite the reader to submit official translations where available.

Broadly, the documents analyzed for this report fall into one of five categories: national strategies and documents by governments,[4] documents from regional and global intergovernmental organizations including member state submissions to the United Nations General Assembly (UNGA), and international private and intergovernmental standards dictionaries. Some of the documents examined did not include terms listed in the Table of Contents and are therefore not cited in this report. The study builds on existing lists of relevant source documents, for example, the European Union Agency for Network and Information Security's – ENISA - webpage listing national cyber security strategies in the world[5] and the database of strategies and policies provided by the NATO Cooperative Cyber Defence Centre of Excellence.[6]

Tables 1-13 provide the number of citations by term and source based on the buckets outlined in the table of contents. Table 14 provides a breakdown by source type for the various definitions.

| **Code** | **Explanation** |
|---|---|
| In paragraph | A definition of the term was supplied in a paragraph either by stating that Term A means X, Y, Z, or by mentioning a term as a definition. |
| Dictionary | The source of this definition was a dictionary. |
| Glossary or specific definition listed in document | A definition of the term was supplied in either a glossary, or in a "Definitions" section of the document. |
| In text box | A definition of the term was supplied outside of the normal text of the document in a text box. |
| Full passage | A term is described in an entire passage. |
| Footnote definition | A term is used in the body of the document and an explicit definition of the term is supplied in a foot or endnote. |

[4] National strategies include national security strategies, national cybersecurity strategies, national information security strategies, national defense strategies, and national military strategies.
[5] European Union. European Union Agency for Network and Information Security, "National Cyber Security Strategies in the World," *ENISA,* Updated 2014. < http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>
[6] North Atlantic Treaty Organization, NATO Cooperative Cyber Defence Center of Excellence, "Strategies & Policies," *NATO CCDCOE,* Updated 2014. <https://www.ccdcoe.org/strategies-policies.html>

# TERMS

## GENERAL

### Computer*

Any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.
**- India, The Information Technology Act, 2008, p. 2**
State > Other (Glossary or specific definition listed in document)

A device or system that is capable of carrying out a sequence of operations in a distinctly and explicitly defined manner. The operations are frequently numerical computations or data manipulations but also include input/output; the operations within the sequence may depend on particular data values. The definition of the sequence is called the program. A computer can have either a stored program or wired program. A stored program may exist in an alterable (read-write or RAM) memory or in a nonalterable (ROM) memory.
**- Oxford University, A Dictionary of Computing, 2004, p. 102**
Other Source (Dictionary)

### Computer System*

"Computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data
**- Council of Europe, Convention on Cybercrime, 2001**
Intergovernmental Organization (Glossary or specific definition listed in document)

One or more interconnected computers with associated software and peripheral devices. It can include sensors and/or (programmable logic) controllers, connected over a computer network. Computer systems can be general purpose (for example, a laptop) or specialized (for example, the “blue force tracking system”).
**- NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare, 2013, p. 258**
Other Source (Glossary or specific definition listed in document)

### Information

1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 175 (JP 3-13.1)**
State > P5 (Glossary or specific definition listed in document)

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 93**
State > P5 (Glossary or specific definition listed in document)

Observation, experience or knowledge about certain facts, objects or phenomena represented in an accessible form which changes, transforms or vitally influences a person's knowledge or set of skills or the way they are organised, and which reduces or eliminates such person's uncertainty.
**- Hungary, Act L of 2013 on Electronic Information Security of Central and Local Government Agencies, 2013, p. 3**
State > OSCE (Glossary or specific definition listed in document)

When we speak of information we are referring, directly or indirectly, to information technology and telecommunication systems (new technologies, new software, new hardware, new ways of elaborating ever more consistent, reliable and speedy information) and, in particular, the risk and security of such systems.
**- Bolivia, Submission to the United Nations General Assembly Resolution A/58/373, p. 2**
State > Other (In paragraph)

Information includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.
**- India, The Information Technology Act, 2008, p. 3**
State > Other (Glossary or specific definition listed in document)

Information refers to any element of knowledge likely to be represented with the aid of devices and to be used, conserved, processed or communicated. Information may be expressed in written, visual, audio, digital and other forms.
**- African Union, Draft African Union Convention on the Establishment of a Credible legal Framework for Cyber Security in Africa, 2012, p. 9**
Intergovernmental Organization (In paragraph)

Intelligence or knowledge capable of being represented in forms suitable for communication, storage or processing. Note - Information may be represented for example by signs, symbols, pictures or sounds.
**- International Telecommunication Union, ITU-R, V662-3, 2000, Ap. 2 § 1 (1.01)**
Intergovernmental Organization (Glossary or specific definition listed in document)

Any kind of knowledge, that is exchangeable amongst users, about things, facts, concepts and so on, in a universe of discourse. Although information will necessarily have a representation form to make it communicable, it is the interpretation of this representation (the meaning) that is relevant in the first place.
**- International Telecommunication Union, ITU-T, X.902, 2009, 3.2.6**
Intergovernmental Organization (Glossary or specific definition listed in document)

Content of communication; data and metadata describing data. The material basis is raw data, which is processed into relevant information. Distributed resource device information categories include source information (e.g., analogue and state information) and derived information (e.g., statistical and historical information).

**- Institute of Electrical and Electronic Engineers, IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems**

Other Source (Dictionary)

1. (I) Facts and ideas, which can be represented (encoded) as various forms of data.
2. (I) Knowledge -- e.g., data, instructions -- in any medium or form that can be communicated between system entities.

Tutorial: Internet security could be defined simply as protecting information in the Internet. However, the perceived need to use different protective measures for different types of information (e.g., authentication information, classified information, collateral information, national security information, personal information, protocol control information, sensitive compartmented information, sensitive information) has led to the diversity of terminology listed in this Glossary.

**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**

Other Source (Glossary or specific definition listed in document)

Generally, information is whatever is capable of causing a human mind to change its opinion about the current state of the real world. Formally,, and especially in science and engineering, information is whatever contributes to a reduction in the uncertainty of the state of a system; in this case, uncertainty is usually expressed in an objectively measurable form. Commonly, this is done by means of Shannon's entropy. Nevertheless, this formula for uncertainty involves probabilities, and these may well have to be subjective. If that is so, the formal measurement must be qualified as depending on subjective probabilities, and "uncertainty" must be replaced by "opinion, or personal estimate, of uncertainty". Information must be distinguished from any medium that is capable of carrying it. A physical medium (such as a magnetic disk) may carry a logical medium (data, such as binary or text symbols). The information content of any physical objects, or logical data, cannot be measured or discussed until it is known what range of possibilities existed before and after they were received. The information lies in the reduction in uncertainty resulting from the receipt of the objects or the data, and not in the size or complexity of the objects or data themselves. Questions of the form, function, and semantic import of data are only relevant to information inasmuch as they contribute to the reduction of uncertainty. If an identical memorandum is received twice, it does not convey twice the information that its first occurrence conveyed: the second occurrence conveys no information at all, unless, by prior agreement, the number of occurrences is itself to be regarded as significant.

Information has ramifications in security, politics, culture, and the economy, as well as in science and engineering. The extent to which information is used as an economic commodity is one of the defining characteristics of the "post-industrial" society, hence the phrase "the information society".

**- Oxford University, A Dictionary of Computing, 2008, p. 250**

**- Oxford University, A Dictionary of Computing, 2004, p. 258**

Other Source (Dictionary)

## Information and Communications Technologies

Any information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.
**- United States of America, National Initiative for Cybersecurity Careers and Studies Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Translation: The set of resources, tools, equipment, computer program applications, networks and media, which enable the compilation, processing, storage, and transmission of information like voice, data, text, video, and images.[i]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 41**
State > UNGGE4 (Glossary or specific definition listed in document)
The applications of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.
**- Kenya, Cybersecurity Strategy, 2014, p. 12**
State > UNGGE4 (Glossary or specific definition listed in document)

ICT is an umbrella term for all computer- (IT) and network- (CT) based technologies as well as related economic sectors. Information and communication technology is also used as a blanket term for all communication instruments or communication applications, including radio, television, mobile telephones, hardware and software for computers and networks, satellite systems, etc. as well as different services and applications related to these items.
**- Austria, Austrian Cyber Security Strategy, 2013, p. 22**
State > OSCE (Glossary or specific definition listed in document)

Australia's national security, economic prosperity and social well being are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies (ICT). This includes desktop computers, the Internet, mobile communications devices and other computer systems and networks.
**- Australia, Cyber Security Strategy, 2009, p. 1**
State > Other (In paragraph)

Technologies and equipment that handle (e.g., access, create, collect, store, transmit, receive, disseminate) information and communication. [in force]
**- International Telecommunication Union, ITU-T K.58 (02/2014), 2014, 3.2.1**
Intergovernmental Organization (Glossary or specific definition listed in document)

## Information System

Organised set of resources (hardware, software, personnel, data and procedures) used to process and circulate information.
**- France, Information Systems Defence and Security: France's Strategy, 2011, p. 22**
State > P5 (Glossary or specific definition listed in document)

The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 176 (JP 3-13)**
State > P5 (Glossary or specific definition listed in document)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 97**
State > P5 (Glossary or specific definition listed in document)

A combination of information concentrated within databases and of information technologies and complex of program and technical means that provide processing of this information.
**- Belarus, Law of the Republic of Belarus "On Information, Informatization and Protection of information", 2008, Article 2**
State > UNGGE4 (Glossary or specific definition listed in document)

A totality of information technologies and documents arranged in organisational and technical respects, including with the use of means of computer engineering technique.
**- Azerbaijan, Law on Information, Informatization and Protection of Information, 1998**
State > OSCE (Glossary or specific definition listed in document)

Information system means the system comprising the personnel, information processing equipment, data transfer equipment and software programs intended to make some operation more efficient, easier or even possible by means of information (data) processing.
**- Finland, Finland's Cyber Security Strategy, 2013, p. 13**
State > OSCE (Glossary or specific definition listed in document)

System for collecting, storing, processing, transmitting and presenting data.
**- Norway, Cyber Security Strategy for Norway, 2012, p. 29**
State > OSCE (Glossary or specific definition listed in document)

The systems involved in providing services, processes and data by means of information and communication technologies.
**- Turkey, National Cyber Security Strategy and 2013-2014 Action Plan, 2013, p. 9**
State > OSCE (Glossary or specific definition listed in document)

Any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.
**- Council of Europe, Council Framework Decision 2005/222/JHA of February 2005 on attacks against information systems, 2005**
Intergovernmental Organization (Glossary or specific definition listed in document)

A system that processes only information.
**- International Telecommunication Union, ITU-T G.800, 2012, 3.2.7**
Intergovernmental Organization (Glossary or specific definition listed in document)

A phrase used to describe all computer and communications systems. [in force]
**- International Telecommunication Union, Recommendation UIT-R REC-SM.668 -1 (03/1997), 1997, An. 10, Ap. 1, & 3**
Intergovernmental Organization (Glossary or specific definition listed in document)

Applications, services, information technology assets, or other information handling components.
**- International Organization for Standardization, ISO/IEC 27000:2014, 2.39**
Other Source (Glossary or specific definition listed in document)

(I) An organized assembly of computing and communication resources and procedures -- i.e., equipment and services, together with their supporting infrastructure, facilities, and personnel -- that create, collect, record, process, store, transport, retrieve, display, disseminate, control, or dispose of information to accomplish a specified set of functions. (See: system entity, system resource. Compare: computer platform.)
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

A computer-based system with the defining characteristic that it provides information to users in one or more organizations. Information systems are thus distinguished from, for example, real-time control systems, message-switching systems, software engineering environments, or personal computing systems. The term could have a very much wider meaning than suggested, considering the meaning of the words information and system. It could, for instance be broadened to include all computer-based systems, or further broadened to include many non-computer-based systems. Thus within the domain of computer-based systems, the more specific term organizational information system is sometimes used. Information systems include data processing applications, office automation applications, and many expert system applications. When their primary purpose is to supply information to management, they are commonly called management information systems.
The following are among the more important characteristics of information systems, and make their design and construction particularly difficult.

(a) Their environment is complex, not fully definable, and not easily modeled.
(b) They have a complex interface with their environment, comprising multiple inputs and outputs.
(c) The functional relationships between inputs and outputs are structurally, if not algorithmically, complex.
(d) They usually include large and complex databases (or, in future, knowledge bases).
(e) Their “host” organizations are usually highly dependent on their continuing availability over very long periods, often with great urgency attending their initial provision or subsequent modification.

**- Oxford University, A Dictionary of Computing, 2008, p. 251**
Other Source (Dictionary)

## Information Technology

Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 100**
State > P5 (Glossary or specific definition listed in document)

(Information Technologies) a combination of processes and methods of search, transmission, receipt, storage, processing, use, distribution and (or) provision of information.
**- Belarus, Law of the Republic of Belarus "On Information, Informatization and Protection of information", 2008, Article 2**
State > UNGGE4 (Glossary or specific definition listed in document)

Translation: Information technology in the context of this law encompasses all technical means to process or transmit information.[ii]
**- Germany, Law to Strengthen the Security of Federal Information Technology, 2009**
State > UNGGE4 (Glossary or specific definition listed in the text)

Methods and systems of means used during information processes, including means of computer engineering technique and communication.
**- Azerbaijan, Law on Information, Informatization and Protection of Information, 1998, Article 2**
State > OSCE (Glossary or specific definition listed in document)

Information technology, encompassing all developments in the field of information and telecommunications, has come to play a vital role in all sectors of society.
**- Brunei Darussalam, Submission to the United Nations General Assembly Resolution A/62/98, p. 2**
State > Other (In paragraph)

Any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.
**- League of Arab States, Arab Convention on Combating Information Technology Offenses, 2010 p. 3**
Intergovernmental Organization (Glossary or specific definition listed in document)

Any form of technology, ie any equipment or technique, sued by people to handle information. Mankind has handled information for thousands of years; early technologies included the abacus and printing. The last four decades or so have seen an amazingly rapid development of information technology, spearheaded by the computer; more recently, cheap microelectronics have permitted the diffusion of this technology into almost all aspects of daily life and an almost inextricable cross-fertilizing and intermingling of its various branches. The term information technology was coined, probably in the late

1970s, to refer to this nexus of modern technology, electronic-based , for handling information. It incorporates the whole of computing and telecommunication technology, together with major parts of consumer electronics and broadcasting. Its applications are industrial, commercial, administrative, educational, medical, scientific, professional, and domestic. The advanced nations have all realized that developing competence in information technology is important, expensive, and difficult; large-scale information technology systems are now economically feasible and there are national programs of research and education to stimulate development. The fundamental capabilities that are usually recognized to be essential comprise VLSI circuit design and production facilities, and a common infrastructure for the storage and transmission of digital information (including digitized voice and image as well as conventional data and text). Major research problems include improved systems and software technology, advanced programming techniques (especially in knowledge-based systems), and improved human-computer interfaces).

**- Oxford University, A Dictionary of Computing, 2008, p. 251**

Other Source (Dictionary)

## Information Technology and Communication

Technologies used to gather, store, use and send information, including technologies that involve the use of computers or any communications system, including any telecommunication system.

**- Economic Community of West African States, Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS, 2009, p. 3**

Intergovernmental Organization (Glossary or specific definition listed in document)

## The Internet*

The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 103**

State > P5 (Glossary or specific definition listed in document)

Translation: Global computer network (network of networks) based on the transmission standard (protocol) TCP/IP. The Internet functions across platforms and operating systems. Characteristic services in the Internet are World Wide Web (WWW) and e-mail.[iii]

**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**

State > UNGGE4 (Glossary or specific definition listed in document)

A collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network.

**- International Telecommunication Union, ITU-T, Y.101, 2000, 37**

Intergovernmental Organization (Glossary or specific definition listed in document)

Global system of inter-connected networks in the public domain.
NOTE There is a difference between the definition of “an internet”[7] and “the Internet”.
**- International Organization for Standardization, ISO/IEC 27032:2012, 2012, 4.29**
Other Source (Glossary or specific definition listed in document)

1. (I) /not capitalized/ Abbreviation of "internetwork".
2. (I) /capitalized/ The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB (RFC 2026) and (b) the name and address spaces managed by the ICANN. (See: Internet Layer, Internet Protocol Suite.)
Usage: Use with definite article ("the") when using as a noun. For example, say "My LAN is small, but the Internet is large." Don't say "My LAN is small, but Internet is large."
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

The global information network that now links a very substantial fraction of the world’s computer networks. The Internet is an extraordinary development that stems for the original ARPANET, which was initiated in North America in 1969. In broad terms the Internet does not offer services to end-users, but servers primarily to interconnect other networks on which end-user services are located. It provides basic services for file transfer, electronic mail, and remote login, and high-level services including he World Wide Web and the MBONE.
The Internet is global, with connections to nearly every country in the world. It is deliberately nonpolitical and tends to deal with nongovernmental levels within a country. The structure is informal, with a minimal level of governing bodies and with an emphasis in these bodies on technical rather than on administration or revenue generation. Up to the mid-1990s the major users of the Internet were the academic and research communities, but over the last decade, with a growth in home computing, there has been a massive increase in the number of individuals and companies using the World Wide Web and electronic mail. There has also been a large increase in commercial interesting in the exploitation of the Internet.
**- Oxford University, A Dictionary of Computing, 2004, p. 269**
Other Source (Dictionary)

[7] “Collection of interconnected networks
NOTE 1 Adapted from ISO/IEC 27033-1:2009
NOTE 2 In this context, reference would be made to ‘an internet’. There is a difference between the definition of ‘an internet’ and ‘the Internet’.” From *ISO/IEC 27032:2012-07-15*

# SPACE

## Cyber Domain

Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures.
**- Finland, Finland's Cyber Security Strategy, 2013, p. 12**
State > OSCE (Glossary or specific definition listed in document)

## 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. [in force]
**- International Telecommunication Union, ITU-T X.1205 (04/2008), 2008, 3.2.4**
Intergovernmental Organization (Glossary or specific definition listed in document)

## Cyber Space

The communication space created by the worldwide interconnection of automated digital data processing equipment.
**- France, Information Systems Defence and Security: France's Strategy, 2011, p. 21**
State > P5 (Glossary or specific definition listed in document)

Translation: A sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form human activity on them (individual, organizational, state).[iv]
**- Russia, Concept Strategy for Cybersecurity of the Russian Federation (Концепция Стратегии Кибербезопасности Российской Федерации), p. 2**
State > P5 (Glossary or specific definition listed in document)

Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.
**- United Kingdom, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, 2011, p. 11**
(In paragraph)

Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.
**- United Kingdom, Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space, 2009, p. 7**
State > P5 (Glossary or specific definition listed in document)

Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.
**- United States of America, The National Strategy to Secure Cyberspace, 2003, p. VII**
State > P5 (In paragraph)

The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security.
**- United States of America, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009, p. III**
State > P5 (Glossary or specific definition listed in document)

A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2014, p. 64 (JP 3-12)**
State > P5 (Dictionary)

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 92 (CJCS CM-0363-08)**
State > P5 (Dictionary)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 58**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 2010, p. 6**
State > P5 (Glossary or specific definition listed in document)

The interdependent network of information technology infrastructures, that includes the Internet, telecommunications network, computer systems, and embedded processors and controllers.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Translation: Is both the physical and virtual environment consisting of computers, computer systems, computer programs (software), telecommunications networks, data and information which is used for the interaction between users.[v]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 38**
State > UNGGE4 (Glossary or specific definition listed in document)

Cyberspace is a public good and a public space. As such, we have to consider cyberspace security in terms of the resilience of infrastructure and the integrity and failure safety of systems and its contained data. Being a public space, States have to promote security in cyberspace, particularly regarding security against crime and malicious activities, by protecting those who choose to use authenticity tools against identity theft and securing the integrity and confidentiality of networks and data. Cyberspace is global by nature. Ensuring cyber security, enforcing rights and protecting critical information infrastructures requires major efforts by the State at the national level and in cooperation with international partners.
**- Germany, Submission to the United Nations General Assembly Resolution A/68/156, 7**
State > UNGGE4 (Full passage)
**- Germany, Submission to the United Nations General Assembly Resolution A/66/152, 9**
State > UNGGE4 (Full passage)

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.
**- Germany, Cyber Security Strategy for Germany, 2011, p. 9**
State > UNGGE4 (Glossary or specific definition listed in document)
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

The physical and non-physical domain that is created or composed of part or all of the following components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data.
**- Israel, Resolution No. 3611: Advancing National Cyberspace Capabilities, 2011, p. 1**
State > UNGGE4 (Glossary or specific definition listed in document)

"Cyberspace," 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 of information, have rapidly expanded and begun permeating real-space.
**- Japan, Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace, 2013, p. 5**
State > UNGGE4 (In paragraph)

Cyberspace, a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities.
**- Japan, National Security Strategy, 2013, p. 9**
State > UNGGE4 (In paragraph)

The notional environment in which communication over computer networks occurs.
**- Kenya, Cybersecurity Strategy, 2014, p. 12**
State > UNGGE4 (Glossary or specific definition listed in document)
**- The Oxford English Dictionary, 2014**
Other Source(Dictionary)

Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology - including the Internet - networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalisation that provides new opportunities but also entails new challenges, risks and threats.
**- Spain, National Cyber Security Strategy, 2013, p. 9**
State > UNGGE4 (In paragraph)

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”.
- **Austria, Austrian Cyber Security Strategy, 2013, p. 21**
State > OSCE (Glossary or specific definition listed in document)

Translation: Cyberspace is the global environment for the interconnection of information and communication systems. Cyberspace is wider than the computer world and also contains computer networks, computer systems, digital media and digital data, whether physical or virtual.[vi]
**- Belgium, Cyber Security Strategy, 2012, p. 12**
State > OSCE (Glossary or specific definition listed in document)

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.
**- Canada, Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada, 2010, p. 2**
State > OSCE (In text box)

Cyber space means digital environment, enabling to create, process, and exchange information, created by information systems and services and electronic communication networks.
**- Czech Republic, Draft Act on Cyber Security, 2014, p. 2**
State > OSCE (Glossary or specific definition listed in document)

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.
**- Hungary, Annex 1 to Government Decision No. 1139/2013 National Cyber Security Strategy of Hungary, 2013, p. 3**
State > OSCE (Glossary or specific definition listed in document)

Cyberspace is a man-made domain essentially composed of ICT nodes and networks, hosting and processing an ever-increasing wealth of data of strategic importance for States, firms, and citizens alike, and for all political, social and economic decision-makers.
**- Italy, 2013 National Strategic Framework for cyberspace security, 2013, p. 9**
State > OSCE (Glossary or specific definition listed in document)

Cyberspace is a global space which has no national boundaries, hence, the rapid spread of threats across cyberspace.
**- Lithuania, Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019, 2011, p. 3**
State > OSCE (Glossary or specific definition listed in document)

Cyberspace is more than Internet; it includes not only hardware, software and information systems, but also the people, social interaction within these networks.
**- Montenegro, National Cyber Security Strategy for Montenegro 2013-2017, 2013, p. 5**
State > OSCE (Glossary or specific definition listed in document)

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.
**- Netherlands, The Defence Cyber Strategy, 2012, p. 4**
State > OSCE (Footnote Definition)

A space of processing and exchanging information created by the ICT systems,[8] together with links between them and the relations with users.
**- Poland, Cyberspace Protection Policy of the Republic of Poland, 2013, p. 5**
State > OSCE (Glossary or specific definition listed in document)

Translation: Cyberspace is characterized by the absence of borders, dynamism, and autonomy, creating opportunities to develop both knowledge-based information society and risks to its operation.[vii]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de secur**
State > OSCE (In paragraph)

Translation: The virtual environment generated by cyber infrastructure, including content information processed, stored, or transmitted, and the actions performed by users in it.[viii]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

The state, the private sector and society make use of information and communication infrastructure and access to cyberspace (Internet, mobile networks and applications, e-business, e-government, computer-based control programmes).
**- Switzerland, National strategy for the protection of Switzerland against cyber risks, 2012, p. 5**
State > OSCE (Glossary or specific definition listed in document)

The environment which consists of information systems that span across the world including the networks that interconnect these systems.
**- Turkey, National Cyber Security Strategy and 2013-2014 Action Plan, 2013, p. 8**
State > OSCE (Glossary or specific definition listed in document)

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.
**- India, National Cyber Security Policy – 2013 (NCSP-2013), 2013, p.1**
State > Other (Full passage)

Cyberspace, as a network using the Transmission Control Protocol/Internet Protocol (TCP/IP) communications protocol, has shown itself to be a fragile and insecure environment which has allowed criminal groups to attack and, on occasion, destroy it, because priority has been given to commercial and marketing objectives.
**- Lebanon, Submission to the United Nations General Assembly Resolution A/62/98, 12**
State > Other (In paragraph)

The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place.
**- New Zealand, New Zealand's Cyber Security Strategy, 2011, p. 12**
State > Other (Glossary or specific definition listed in document)

[8] As defined by Act of 17 February 2005 on the informatization of entities performing public tasks.

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.
**- South Africa, Notice of Intention to make South African National Cybersecurity Policy, 2010, p. 12**
State > Other (Glossary or specific definition listed in document)

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.
**- NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare, 2013, p. 258**
Other Source (Glossary or specific definition listed in document)

Cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed and deleted.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 17**
Other Source (Glossary or specific definition listed in document)

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.
**- International Organization for Standardization, ISO/IEC27032:2012, Introduction**
Other Source (Glossary or specific definition listed in document)

An informal word first thought to have been used by novelist William Gibson to refer to the total data on all computers on all the networks in the world. The word has passed into common use as a way of referring to any large collection of network-accessible computer-based data.
**- Oxford University, A Dictionary of Computing, 2008, p. 121**
**- Oxford University, A Dictionary of Computing, 2004, p. 125**
Other Source (Dictionary)

## Information Area

The sphere of activity involving the creation, transformation or use of information, including individual and social consciousness, the information and telecommunications infrastructure, and information itself.
**- Russia, Submission to the United Nations General Assembly Resolution A/55/140, 3**
State > P5 (Glossary or specific definition listed in document)

## Information Environment

Aggregate of individuals, organizations, and/or systems that collect, process, or disseminate information, also included is the information itself.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 93**
State > P5 (Glossary or specific definition listed in document)

Information environment is assessed in the following three aspects:
1. Physical aspect includes command and control systems, supporting infrastructure and soldiers who accomplish operations in physical area;
2. Information aspect is the information which is collected, processed, stored, disseminated and protected. Information aspect also includes the cyberspace. This aspect connects physical and cognitive aspects;

3. Cognitive aspect includes those who take decisions and the target audience. The commander and his staff make plans and take decisions. These decisions affect personnel of the adversary or third parties. Cognitive aspect may influence the end-state of war, which is influenced by such factors as leadership, morale, readiness of military unites and individuals, experience, situation awareness, public opinion, media and rumours.

**- Lithuania, Lithuanian Military Doctrine, 2010, p. 51**
State > OSCE (Full passage)

## Information Space

Translation: Activities associated with the formation, creation, conversion, transfer, use, or storage of information that impacts individual and social consciousness, the information infrastructure, and information itself.[ix]

**- Russia, Concept Strategy for Cybersecurity of the Russian Federation (Концепция Стратегии Кибербезопасности Проссийской Федерации), p. 2**
State > P5 (Glossary or specific definition listed in document)

**- Russia, Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве), 2011**
State > P5 (Glossary or specific definition listed in document)

Information Architecture is the (human-centered) structure of an information space and the semantics for accessing required task objects, system objects and other information. The appropriate combination of organization, labelling, navigation schemes and retrieval mechanisms within an information space will facilitate task completion and efficient access to content.

**- International Organization for Standardization, ISO/IEC TR 25060: 2010, 2.8**
Other Source (Glossary or specific definition listed in document)

Information Space is any medium, through which information is created, transmitted, received, stored, processed or deleted.

**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 23**
Other Source (Glossary or specific definition listed in document)

## Information Sphere

The present stage in societal development is characterized by an increasing role of the information sphere, which represents an assemblage of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, and a system governing public relations arising out of these conditions.

**- Russia, Information Security Doctrine of the Russian Federation, 2000, p. 1**
State > P5 (Glossary or specific definition listed in document)

The InfoSphere is the environment where information exists and flows in both structured and/or random ways and where facts or knowledge reside and are represented or conveyed by a particular sequence of symbols, impulses or characterisations.

**- South Africa, South African Defence Review 2012, 2012, p. 172**
State > Other (Full passage)

# SECURITY

## Computer Security*

The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 73 (JP 6-0)**
State > P5 (Dictionary)

Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 41**
State > P5 (Glossary or specific definition listed in document)

Protection of digital computer-based systems throughout the development lifecycle of the system to prevent unauthorized, unintended, and unsafe modifications to the system; this includes protection of the safety system during operation and maintenance from inadvertent actions that result in unintended consequences.
**- Institute for Electronic and Electrical Engineers, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2010**
Other Source (Glossary or specific definition listed in document)

Protection of information, system resources, and system services through controls provided by hardware and software mechanisms, including access controls, user authentication mechanisms, and audit facilities.
**- Institute for Electronic and Electrical Engineers, IEEE Recommended for Practice for Futurebus+, 1993**
Other Source (Glossary or specific definition listed in document)

1. (I) Measures to implement and assure security services in a computer system, particularly those that assure access control service.
Usage: Usually refers to internal controls (functions, features, and technical characteristics) that are implemented in software (especially in operating systems); sometimes refers to internal controls implemented in hardware; rarely used to refer to external controls.
2. (O) "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)."
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Cyber Security

The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence.
**- France, Information Systems Defence and Security: France's Strategy, 2011, p. 21**
State > P5 (Glossary or specific definition listed in document)

Translation: A set of conditions under which all components of cyberspace are protected from the maximum number of threats and impacts with undesirable consequences.[x]
**- Russia, Concept Strategy for Cybersecurity of the Russian Federation (Концепция Стратегии Кибербезопасности Российской Федерации), p. 2**
State > P5 (Glossary or specific definition listed in document)

Cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers. It is important to remember that cyber security is not an end in itself. It should not discourage the use of new technologies. The Government's Digital Britain Strategy aims to make the UK the leading major economy for innovation, investment and quality in the digital and communications industries. The Government's ultimate goal is to enable the full benefits of cyber space for the UK.
**- United Kingdom, Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space, 2009, p. 9**
State > P5 (Full passage)

Cyber security refers to defenses against electronic attacks launched via computer systems.
**- United Kingdom, Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK, 2011, p. 1**
State > P5 (In Paragraph)

The ability to protect or defend the use of cyberspace from cyber attacks.
**- United States of America, Committee on National Security Systems National Information Assurance Glossary, 2010, p. 22**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 58**
State > P5 (Glossary or specific definition listed in document)

Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.
**- United States of America, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009, p. iii**
State > P5 (Full passage)

The process of protecting information by preventing, detecting, and responding to attacks.
**- United States of America, Framework for Improving Critical Infrastructure Cybersecurity, 2014, p. 37**
State > P5 (Glossary or specific definition listed in document)

Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Translation: Capacity of the state to minimize the risks they and their citizens are exposed to, in the face of threats and incidents of the cyber nature.[xi]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 39**
State > UNGGE4 (Glossary or specific definition listed in document)

It is an essential precondition for the securing of cyberspace that every operator of a computer, computer network or information system realises the personal responsibility of using the data and instruments of communication at his or her disposal in a purposeful and appropriate manner. Estonia's cyber security strategy seeks primarily to reduce the inherent vulnerabilities of cyberspace in the nation as a whole.
**- Estonia, Cyber Security Strategy, 2008, p. 3**
State > UNGGE4 (Full passage)

(Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace.
**- Germany, Cyber Security Strategy for Germany, 2011, p. 15**
State > UNGGE4 (Full passage)
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Full passage)

Translation: Cybersecurity expands the area of activity of classic IT security to cover the entire cyberspace. The latter encompasses all information technology connecting with the Internet or comparable networks including cyberspace-based communication, applications, processes, and processed information. Thereby, for all intents and purposes, the entire modern information and communications technology becomes part of cyberspace.[xii]
**- Germany, Federal Office for Information Security (BSI): Cybersecurity**
State > UNGGE4 (In paragraph)

Our vision is to secure the Critical National Information Infrastructure (CNII) and make it resilient, and for Ghana to be self-reliant in securing its cyber space by infusing a culture of security to promote stability, social well being and wealth creation of our people. All actors in law enforcement, national security, network security practitioners in government and business, and the public will take part in the vision.
**- Ghana, Making our Cyber Space Safe, 2014, p. 14**
State > UNGGE4 (In paragraph)

Policies, security arrangements, actions, guidelines, risk management protocols and technological tools designated to protect cyberspace and allow action to be taken therein.
**- Israel, Resolution No. 3611: Advancing National Cyberspace Capabilities, 2011, p. 1**
State > UNGGE4 (Glossary or specific definition listed in document)

Japan aims to construct a "world-leading," "resilient" and "vigorous" cyberspace, and incorporate this cyberspace as a social system to realize a "cybersecurity nation" as a society that is strong against cyber attacks, full of innovations and of which its people will be proud.
**- Japan, Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace, 2013, p. 19**
State > UNGGE4 (In paragraph)

The processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction.
**- Kenya, Cybersecurity Strategy, 2014, p. 12**
State > UNGGE4 (Glossary or specific definition listed in document)

The term "cyber security" refers to organisations, institutions or persons with a vested interest in cyber security, or particularly severely affected by it.
**- Austria, National ICT Security Strategy Austria, 2012, p. 6, 2013, p. 6**
State > OSCE (In Paragraph)

Cyber security describes the protection of a key legal asset through constitutional means against actor-related, technical, organisational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cyber security helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimise the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services.
**- Austria, Austrian Cyber Security Strategy, 2013, p. 21**
State > OSCE (Glossary or specific definition listed in document)

Translation: Cybersecurity is the desired situation or protection of cyberspace and is proportional to the cyber threat and potential consequences of cyber attacks. In a situation of cyber security, disruption, attack, or misuese of ICT does not cause any danger or harm. The consequences of abuse, disruption or attack may include restricting availability and reliability of ICT, the violation of the confidentiality of information, or the damaging of the integrity of information (addition, deletion, or modification [of information] are illegal).[xiii]
**- Belgium, Cyber Security Strategy, 2012, p. 12**
State > OSCE (Glossary or specific definition listed in document)

Cyber security means a complex of legal, organizational, technical and educational means ensuring the protection of cyber space.
**- Czech Republic, Draft Act on Cyber Security, 2014, p. 2**
State > OSCE (In paragraph)

Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured.
**- Finland, Finland's Cyber Security Strategy, 2013, p. 13**
State > OSCE (In paragraph)

The security of cyber space and the protection of electronic information is very important for Georgia. As information technologies rapidly evolve, critical infrastructure is becoming more dependent on them. Therefore, combating cyber crime and protecting against cyber attacks is very important to the national interests of Georgia.
**- Georgia, National Security Concept of Georgia, 2011, p. 5**
State > OSCE (In paragraph)

The ongoing and systematic application of political, legal, economic, educational, awareness-raising and technical tools suitable for managing cyberspace risks, transforming the cyberspace into a reliable environment by ensuring an acceptable level of such risks for the smooth functioning and operation of social and economic processes.
**- Hungary, Act L of 2013 on Electronic Information Security of Central and Local Government Agencies, 2013, p. 3**
State > OSCE (Glossary or specific definition listed in document)

Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace.
**- Hungary, Annex 1 to Government Decision No. 1139/2013 National Cyber Security Strategy of Hungary, 2013, p. 3**
State > OSCE (In paragraph)

The present National Cybersecurity Strategic Framework and the related National Plan, both foreseen by the Prime minister's "Decree Containing Strategic Guidelines for the National Cyber Protection and ICT Security" of the 24th January 2013, aim at enhancing the national preparedness to respond to present and future challenges affecting cyberspace, and are devoted to directing all national efforts toward common and agreed solutions, knowing that cybersecurity is a process rather than an end to itself, that technical innovations will always introduce new vulnerabilities in the strategic and operational horizon, and that the intrinsic nature of cyber threats makes our defence, at least for the time being, mostly - although not exclusively - reactive.
**- Italy, 2013 National Strategic Framework for cyberspace security, 2013, p. 12**
State > OSCE (In paragraph)

Electronic information security (cyber security).
**- Lithuania, Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019, 2011, p. 1**
State > OSCE (In paragraph)

International Standardisation Organisation (ISO) defines cyber security as “preservation of confidentiality, integrity and availability of information in cyberspace”. The Netherlands have offered a little broader definition: “freedom from danger or damage caused by disruption, failure or abuse of ICT systems” Danger or damage caused by disruption, failure or abuse may consist of a limitation in the availability or reliability of ICT systems, a breach of the confidentiality stored in them, or damage to the integrity of the information. ITU also defines broadly the cyber security: “collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user’s assets. Cyber security seeks to ensure the attainment and maintenance of the security properties of the organisation and user’s assets against relevant security risks in the cyber environment. General security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality”.
**- Montenegro, National Cyber Security Strategy for Montenegro 2013-2017, 2013, p. 6**
State > OSCE (Full passage)

Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.
**- Netherlands, National Cyber Security Strategy 2: From awareness to capability, 2013, p. 7**
State > OSCE (In paragraph)

Protection of data and systems connected to the Internet.
**- Norway, Cyber Security Strategy for Norway, 2012, p. 28**
State > OSCE (Glossary or specific definition listed in document)

Translation: The state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information electronically for public and private resources and services in cyberspace. Proactive and reactive measures may include policies, concepts, standards and guidelines for security, risk management, training and awareness activities, implementing technical solutions to protect cyber infrastructure, identity management, and consequence management.[xiv]

**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 7**

State > OSCE (Glossary or specific definition listed in document)

Sweden will mainly use the term 'cybersecurity' and related concepts, signifying efforts aimed at the preservation of the confidentiality, availability and integrity of information in electronic communications networks and IT systems.

**- Sweden, Submission to the United Nations General Assembly Resolution A/68/243, p. 2**

State > OSCE (In paragraph)

Protection of information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information being processed in this space, detection of attacks and cyber security incidents, putting into force the countermeasures against these incidents and then putting these systems back to their states previous to the cyber security incident.

**- Turkey, National Cyber Security Strategy and 2013-2014 Action Plan, 2013, p. 9**

State > OSCE (Glossary or specific definition listed in document)

Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.

**- Australia, Cyber Security Strategy, 2009, p. 5**

State > Other (Glossary or specific definition listed in document)

The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.

**- New Zealand, New Zealand's Cyber Security Strategy, 2011, p. 12**

State > Other (Glossary or specific definition listed in document)

The ability to protect or defend the use of cyberspace from cyber-attacks.

**- Saudi Arabia, Developing National Information Security Strategy for the Kingdom of Saudi Arabia, 2013, p. A-2**

State > Other (Glossary or specific definition listed in document)

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protected the cyber environment and organization and user assets. Organisation and user's assets include connecting computing devices, personnel, infrastructure, applications, services, telecommunication systems, and a totality of transmitted and/or stored information in the cyber environment.

**- South Africa, Notice of Intention to make South African National Cybersecurity Policy, 2010, p. 12**

State > Other (In paragraph)

To build a secure and resilient cyberspace for citizens, businesses and Government. To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.
**- India, National Cyber Security Policy – 2013 (NCSP-2013), 2013, p. 3**
State > Other (In paragraph)

Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
**- India, The Information Technology Act, 2008, p. 3**
State > Other (Glossary or specific definition listed in document)

Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.
**- European Union, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, p. 3**
Intergovernmental Organization (In paragraph)

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, and confidentiality. [in force]
**- International Telecommunication Union, ITU-T X.1205 (04/2008), 2008, 3.2.5**
Intergovernmental Organization (Glossary or specific definition listed in document)

The protection of data and systems in networks that are connect to the Internet. [in force]
**- International Telecommunication Union, ITU-T, Rec. E.800 (09/2008), 2008, 3.1.3.23**
Intergovernmental Organization (Glossary or specific definition listed in document)

Cybersecurity is a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 33**
Other Source (Glossary or specific definition listed in document)

The vulnerability of any computing system, software program, or critical infrastructure, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems.
**- Institute for Electronic and Electrical Engineers, IEEE Standard Criteria for Security Systems for Nuclear Power, 2010**
Other Source (Glossary or specific definition listed in document)

"Cybersecurity" or "Cyberspace security" [is], defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace".
**- International Organization for Standardization, ISO/IEC 27032:2012**
Other Source (Glossary or specific definition listed in document)

Preservation of confidentiality, integrity and availability of information in the Cyberspace.
**- International Organization for Standardization, ISO/IEC 27032:2012**
Other Source (Glossary or specific definition listed in document)

As a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and "solutions" ranging from the technical to the legislative. While buzzwords like cybersecurity may make for good headlines, serious discussions of security and the Internet require a shared understanding of what is meant by cybersecurity.
**- Internet Society, Some Perspectives on Cybersecurity: 2012, p. 1**
Other Source (In paragraph)

The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
**- The Oxford English Dictionary, 2014**
Other Source (Dictionary)

## Information Security

It is the view of China that the problem of information security not only involves the risks arising from the weakness of the basic information infrastructure, but also the political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology. Each of these two factors is worthy of equal concern when studying the problem of information security.
**- China, Submission to the United Nations General Assembly Resolution A/61/161, p. 4**
State > P5 (In paragraph)

It is the view of China that the issue of information security involves not only the risks arising from the weakness and interconnected nature of the basic information infrastructure, but also the political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology. Both of these factors are worthy of concern when studying the issue of information security.
**- China, Submission to the United Nations General Assembly Resolution A/62/98, p. 7**
State > P5 (In paragraph)

Protection of the basic interests of the individual, society and the State in the information area, including the information and telecommunications infrastructure and information per se with respect to its characteristics, such as integrity, objectivity, accessibility and confidentiality.
**- Russia, Submission to the United Nations General Assembly Resolution A/54/213, p. 10**
State > P5 (Glossary or specific definition listed in document)

A situation in which the basic interests of the individual, of society and of the State in the information area, including the information and telecommunications infrastructure and information itself with respect to its characteristics such as integrity, objectivity, availability and confidentiality, are protected.
**- Russia, Submission to the United Nations General Assembly Resolution A/55/140, p. 3-4**
State > P5 (Glossary or specific definition listed in document)

Translation: The state of security for the individual, organizations, and the state and its interests, from the threats and other destructive, negative impacts of information space.[xv]

**- Russia, Concept Strategy for Cybersecurity of the Russian Federation (Концепция Страгегии Кибербезопасности Проссийской Федерации), p. 2**

State > P5 (Glossary or specific definition listed in document)

By the information security of the Russian Federation is meant the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state.

The interests of the individual in the information sphere consist of the exercise of the constitutional rights of man and the citizen to information access, to use of information in the interest of carrying on activities not prohibited by law and of physical, spiritual and intellectual development, as well as of the protection of information that ensures personal security.

The interests of society in the information sphere consist of securing the interests of the individual in this sphere, reinforcing democracy, creating a rule-of-law social state, achieving and maintaining public harmony and of the spiritual renewal of Russia.

The state's interests in the information sphere consist of creating conditions for harmonious Russian information infrastructure development and for the exercise of the constitutional rights and freedoms of man and the citizen with respect to receiving and using information to ensure the inviolability of the constitutional system, the sovereignty and territorial integrity of Russia, and political, economic and social stability; the interests of the state also consist in the unconditional maintenance of law and order and in the promotion of equal and mutually advantageous international cooperation.

Based on the national interests of the Russian Federation in the information sphere, the state forms its strategic and current domestic and foreign policy objectives for ensuring information security.

**- Russia, Information Security Doctrine of the Russian Federation, 2000, p. 2**

State > P5 (Full passage)

3. Information security encompasses the need to protect scientific research of a commercial character, as well as production technology and other types of proprietary data (e.g., marketing plans and customer service information).

4. Information security is also associated with the need to enforce international agreements on intellectual property (such as video and audio material, as well as computer software), so as to protect it from unauthorized copying and sale. Protection of privacy is yet another aspect of information security, that is, ensuring the security of personal and commercial information transmitted via the public international network or over private data links."

**- United Kingdom, Submission to the United Nations General Assembly Resolution A/54/213, p. 12**

State > P5 (Full Passage)

The United Kingdom will use its preferred terminology of "cybersecurity" and related concepts in the present submission, denoting efforts aimed at the preservation of the confidentiality, availability and integrity of information in cyberspace. The term "information security" is often used by business and standards organizations to mean the same thing, and the term is also accepted by the United Kingdom with this specific meaning. There is scope for potential confusion in the use of the term "information security" in that it is used by some countries and organizations as part of a doctrine that regards information itself as a threat against which additional protection is needed. The United Kingdom does not recognize the validity of the term "information security" when used in this context, since it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

**- United Kingdom, Submission to the United Nations General Assembly Resolution A/68/156, p. 15**

State > P5 (Full passage)

The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 175-176 (Jp 3-13)**
State > P5 (Dictionary)

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 94**
State > P5 (Glossary or specific definition listed in document)

Translation: The state of the protection of balanced interests of the individual, society, and the state from external and internal threats in the information space.[xvi]
**- Belarus, Concept of National Security of the Republic of Belarus, 2010**
State > UNGGE4 (Glossary or specific definition listed in document)

The regular updating of security measures is yet another important aspect of developing information security. The current and well known security objectives – confidentiality, availability and integrity of information – are no longer sufficient to ensuring cyber security. To secure the critical infrastructure, it is necessary also to address the severity of disturbances in its functioning, non-repudiation and authenticity of information sources. Further, ensuring cyber security also involves fields that have so far received little attention, such as physical protection measures to combat electronic attacks against information and communications systems.
**- Estonia, Cybersecurity Strategy, 2008**
State > UNGGE4 (In paragraph)

The role of an information security is to make the IT infrastructure truly dependable and solid within the framework of national objectives of Japan, as a major economic power; specifically, to maintain continuous development, to achieve better lives for the people through the use and utilization of IT, and to ensure national security from a new perspective.
**- Japan, The First National Strategy on Information Security, 2006, p. 4-5**
State > UNGGE4 (In paragraph)

Specifically this is to define the information security "To make the IT infrastructure as to be truly reliable and rigid" concerning 1) sustainable development through the use of IT, 2) achievement higher quality of life of people through the use of IT, 3) security against the threats related to the use of IT.
**- Japan, The Second National Strategy on Information Security, 2009, p. 4-5**
State > UNGGE4 (In paragraph)

The Concept of Information Security was adopted by Order of the President of the Republic of Armenia No. NK-97 of 25 June 2009. It states that the national security of the Republic of Armenia depends considerably on information security, which encompasses components such as information, communication and telecommunication systems.
**- Armenia, Submission to the United Nations General Assembly Resolution A/68/156 add.1, p. 2**
State > OSCE (In paragraph)

Information security or network security are umbrella terms for ICT security, referring to the entire relevant information of an organisation or an enterprise, including information that has not been processed electronically. Hence, it describes the entirety of characteristics of an organisation ensuring the

confidentiality, availability and integrity of information. Information may be available as spoken text, paper documents or other directly readable media or as electronically processed data in ICT systems.
- **Austria, Austrian Cyber Security Strategy, 2013, p. 23**
State > OSCE (In paragraph)

Information security means the administrative and technical measures taken to ensure the availability, integrity and confidentiality of data.
**- Finland, Finland's Cyber Security Strategy, 2013, p. 13**
State > OSCE (Glossary or specific definition listed in document)

Information security includes the state of confidentiality, integrity and availability of information. Information security is focused on data regardless of their form: electronic, printed and other forms of data.
**- Montenegro, National Cyber Security Strategy for Montenegro 2013-2017, 2013, p. 5**
State > OSCE (Glossary or specific definition listed in document)

Protection of the confidentiality, integrity and availability of information.
**- Norway, Cyber Security Strategy for Norway, 2012, p. 28**
State > OSCE (Glossary or specific definition listed in document)

Translation: Information security means protection of systems, data, and infrastructure in order to preserve confidentiality, integrity, and availability of information.[xvii]
**- Serbia, Стратегију развоја информационог друштва у Републици Србији до 2020. Године, 2010, p. 23**
State > OSCE (In paragraph)

In this context the term "information security" must be understood as the kind of protection of a State's information space that allows the attainment of its national interests and observance of the rights of the individual, society and the State.
**- Ukraine, Submission to the United Nations General Assembly Resolution A/58/373, p. 15**
State > OSCE (In paragraph)

Within the security system of Ukraine as a whole, information security holds a special position, as information relations and processes are component parts of all processes within society and the State. In this context, information security is defined as the status of the information space (environment), which consists of information technologies; information resources and the information relations among the relevant actors, that guarantees the evolution and use of the information space for the benefit of the individual, society and the State.
**- Ukraine, Submission to the United Nations General Assembly Resolution A/68/156, p. 11**
State > OSCE (In paragraph)

The objective of information security, as defined in the OECD Guidelines for the Security of Information Systems and used by Australia, is: "… the protection of the interests of those relying on information systems from harm resulting from the failure of availability, confidentiality and integrity".
**- Australia, Submission to the United Nations General Assembly Resolution A/54/213, p. 2**
State > Other (In paragraph)

Information security is related to the concept of national security and the information security system has a direct connection with telecommunications security since it is through telecommunications that information is transmitted and exchanged through networks, whether wired or wireless.
**- Jordan, Submission to the United Nations General Assembly Resolution A/61/161, p. 5**
State > Other (In paragraph)

The nation needs secure and reliable national information infrastructures which are resilient to malicious attack or arbitrary disruption to maintain a high level of trust in these systems across government, with the private sector, and within the citizenry. (In paragraph)
**- Jordan, National Information Assurance and Cyber Security Strategy, 2012, p. 4**
State > Other (In paragraph)

Information security means the situation where conditions are ensured for the Government to assess objectively the country's actual internal and external situation and make correct decisions, for government organs and the people to have the necessary information for the exercise of their powers and rights provided by the Constitution and for the dissemination abroad of information about Mongolia.
**- Mongolia, The Concept of National Security of Mongolia**
State > Other (In paragraph)

In connection with basic notions related to information security, the regulations in effect in the Sultanate, and especially the copyright regulations, characterize information as having material and moral value and thus provide it with legal protection. By means of this principle, it is possible to define the basic notions relating to information security. The most important are as follows:

(a) Illicit interception of information and data;
(b) Illicit entry to computer systems;
(c) Spying and eavesdropping on data and information;
(d) Violation of the privacy of others or of their right to confidentiality;
(e) Provision of data or electronically stored protection systems, and recommend that Member States adopt documents of whichever kind;
(f) Destruction, alteration and diversion of data;
(g) Collection and diversion of information;
(h) Leaking of information and data;
(i) Trespass on computer programs by modification or counterfeiting;
(j) Illicit copying of programs in violation of intellectual property rights;
(k) Theft and use of network addresses;
(l) Alteration, augmentation or deletion of information in an original message in transmission before it reaches the addressee;
(m) Introduction of viruses and tampering with network content;
(n) Actual (physical) destruction of equipment and buildings.

**- Oman, Submission to the United Nations General Assembly Resolution A/54/213, p. 6**
State > Other (In paragraph)

The basic notions for promoting security are those steps that have to be followed to ensure ways and means for the communication of information, as well as the challenges that take place unexpectedly, as illustrated in tables 1 and 2 below, which list the necessary steps at all stages to ensure the security of information, in addition to the new challenges in that respect.
**- Qatar, Submission to the United Nations General Assembly Resolution A/54/213, p. 7**
State > Other (In paragraph)

Information security is the protection information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It is in this regard that the Ministry of Information and Communications Technology whose mandate is to provide strategic and technical leadership, overall coordination, support and advocacy on all matters of policy, laws, regulations and strategy in all matters of ICT in consultation with various stakeholders has developed a National Information Security Strategy to address the information security issues at national level.
**- Uganda, National Information Security Strategy, 2011, p. 6**
State > Other (In paragraph)

Information security, then, has a twofold character, inasmuch as it relates both to the guaranteeing of the protection and defence of the information and to its proper use and veracity. Both the illicit use and the deliberate non-use of information and telecommunication systems or information resources for purposes of destabilization constitute disrupting factors in the context of international security.
**- Venezuela, Submission to the United Nations General Assembly Resolution A/59/116/Add.1, p. 6**
State > Other (In paragraph)

Information Security is property of information space that is an ability to resist threats and respond and recover.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 55**
Other Source (Glossary or specific definition listed in document)

Preservation of confidentiality, integrity and availability of information
Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
**- International Organization for Standardization, ISO/IEC 27000:2014, 2.33**
Other Source (Glossary or specific definition listed in document)

(N) Measures that implement and assure security services in information systems, including in computer systems (see: COMPUSEC) and in communication systems (see: COMSEC).
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Information System Security

All technical and non-technical protective measures enabling an information system to withstand events likely to compromise the availability, integrity or confidentiality of stored, processed or transmitted data and of the related services that these systems offer or make accessible.
**- France, Information Systems Defence and Security: France's Strategy, 2011, p. 22**
State > P5 (Glossary or specific definition listed in document)

## Information Technology (IT) Security*

Translation: IT security describes the condition in which the risks, which exist in the usage of information technology due to threats and vulnerabilities, are reduced through appropriate measures to an acceptable level. IT security is therefore the condition in which availability, integrity, and confidentiality of information and information technology are protected by adequate measures.[xviii]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

Translation: IT security is the condition in which availability, integrity, and confidentiality of information and information technology are protected by adequate measures.[xix]
**- Germany, Implementation Plan KRITIS, 2007**
State > UNGGE4 (Glossary or specific definition listed in the text)

Translation: Security in information technology in the context of this law means the adherence to specific security standareds regarding the availability, integrity, and confidentiality of information through security measures. 1. In information technology systems, components, or processes, or 2. In the usage of information technology systems, components, or processes.[xx]

**- Germany, Law to Strengthen the Security of Federal Information Technology, 2009**
State > UNGGE4 (Glossary or specific definition listed in the text)

## International Information Security

Translation: The state of international relations in which global stability is not disturbed nor is the security of the world community endangered in the information space.[xxi]

**- Russia, Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве), 2011**
State > P5 (Glossary or specific definition listed in document)

International information security should be based on existing international law (jus ad bellum), which defines how to counter threats to international peace and security, and international humanitarian law (jus in bello), which relates to the means and methods of warfare; the protection of States that are not party to the conflict; and persons and property that are or could be affected by the conflict.

**- Mali, Submission to the United Nations General Assembly Resolution A/64/129/Add.1, p. 7**
State > Other (In paragraph)

## Internet Security

Internet security in technical context, refers to "protection of Internet service and related ICT systems and networks as extension of network security in organisations and homes, and to ensure the security purpose". Internet security also provides availability and reliability of Internet service. However, in political context, Internet security is often equated with what is also known as safe use of the Internet. According to some definitions, Internet security includes a global regime dealing with stability of Internet code and hardware, as well as with agreements on prosecuting illegal content. Network security is also important for critical infrastructures that are often not directly connected to the Internet.

**- Montenegro, National Cyber Security Strategy for Montenegro 2013-2017, 2013, p. 6**
State > OSCE (Glossary or specific definition listed in document)

## Security*

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 173**
State > P5 (Glossary or specific definition listed in document)

The protection of information availability, integrity and confidentiality.
**- International Telecommunication Union, Recommendation ITU-R M.1224 (03/2012), 2012, 4.1**
Intergovernmental Organization (Glossary or specific definition listed in document)
**- International Telecommunication Union, Y.140.1 (04), 2004, 3.9**
Intergovernmental Organization (Glossary or specific definition listed in document)

The ability to prevent fraud as well as the protection of information availability, integrity and confidentiality.
**- International Telecommunication Union, Q.1741.1 (04/2002), 2002, 3.32**
Intergovernmental Organization (Glossary or specific definition listed in document)

Property of a system by which confidentiality, integrity, availability, accountability, authenticity, and reliability are achieved.
**- International Organization for Standardization, ISO/IEC TR 15443-1:2012, 2012, 3.21**
Other Source (Glossary or specific definition listed in document)

The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them.
**- International Organization for Standardization, ISO/IEC TR 15443-1:2012, 3.22**
Other Source (Glossary or specific definition listed in document)

1a. (I) A system condition that results from the establishment and maintenance of measures to protect the system.
1b. (I) A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss. (Compare: safety.)
2. (I) Measures taken to protect a system.

Tutorial: Parker suggests that providing a condition of system security may involve the following six basic functions, which overlap to some extent:
- "Deterrence": Reducing an intelligent threat by discouraging action, such as by fear or doubt. (See: attack, threat action.)
- "Avoidance": Reducing a risk by either reducing the value of the potential loss or reducing the probability that the loss will occur. (See: risk analysis. Compare: "risk avoidance" under "risk".)
- "Prevention": Impeding or thwarting a potential security violation by deploying a countermeasure.
- "Detection": Determining that a security violation is impending, is in progress, or has recently occurred, and thus make it possible to reduce the potential loss. (See: intrusion detection.)
- "Recovery": Restoring a normal state of system operation by compensating for a security violation, possibly by eliminating or repairing its effects. (See: contingency plan, main entry for "recovery".)
- "Correction": Changing a security architecture to eliminate or reduce the risk of reoccurrence of a security violation or threat consequence, such as by eliminating a vulnerability.

**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

Prevention of or protection against (a) access to information by unauthorized recipients or (b) intentional but unauthorized destruction or alteration of that information. Security may guard against both unintentional as well as deliberate attempts to access sensitive information, in various combinations according to circumstances. The concepts of security, integrity, and privacy are interlinked.
**- Oxford University, A Dictionary of Computing, 2004, p. 468**
Other Source (Dictionary)

## Security of Information

Security of information means ensuring confidentiality, integrity and availability of information.
**- Czech Republic, Draft Act on Cyber Security, 2014, p. 2**
State > OSCE (Glossary or specific definition listed in document)

Security of information includes the protection of its confidentiality (information should be accessible only to those who are entitled to use it), protection of information against unauthorized modification (integrity), and protection of systems against denial of services (availability) and against unauthorized access.
**- Cuba, Submission to the United Nations General Assembly Resolution A/54/213, p. 4**
State > Other (In paragraph)

# INCIDENT

## Cyber Incident

Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.
**- United States of America, CNSS National Information Assurance Glossary, 2010, p. 22**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 57**
State > P5 (Glossary or specific definition listed in document)

Cyber security incident means a cyber security event during which security of information in information systems breach or security of services or security and integrity of electronic communication networks breach occurred.
**- Czech Republic, Draft Act on Cyber Security, 2014, p. 2**
State > OSCE (Glossary or specific definition listed in document)

Incident shall mean an event, act or omission which gives rise or may give rise to an unauthorized access to an information system or electronic communications network, disruption or change of the operation (including takeover of control) of an information system or electronic communications network, destruction, damage, deletion or the change of electronic information, removal or limiting of the possibility to use electronic information and, also, which gives rise or may give rise to the appropriation, publication, dissemination or any other use of non-public electronic information by persons unauthorized to do so.
**- Lithuania, Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019, 2011, p. 1**
State > OSCE (Glossary or specific definition listed in document)

Translation: An event occurring in cyberspace whose consequences affect cybersecurity.[xxii]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as a computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems.
**- India, National Cyber Security Policy – 2013 (NCSP-2013), 2013, p. 2**
State > Other (In paragraph)

## Information and Communication Networks (ICN) Security Incident

Any real or suspected adverse event in relation to the security of ICN. This includes:
- Intrusion into ICN computer systems via the network;
- Occurrence of computer viruses;
- Probes for vulnerabilities via the network into a range of computer systems
- PABX call leak-through;
- Any other undesired events arising from unauthorized internal or external actions.

**- International Telecommunication Union, ITU-T, E.409, 2004, 1.2.4**
Intergovernmental Organization (Glossary or specific definition listed in document)

## Information Incident

Translation: Any adverse event, real or suspected, in relation to the security of computer systems or computer networks.[xxiii]

**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 39**
State > UNGGE4 (Glossary or specific definition listed in document)

## Information Security Event*

Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.

**- International Organization for Standardization, ISO/IEC 27035:2011-09-01, 2011, 3.3**
Other Source (Glossary or specific definition listed in document)

**- International Organization for Standardization, ISO/IEC 27000:2014-01-15, 2014, 2.35**
Other Source (Glossary or specific definition listed in document)

## Information Security Incident*

Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

**- International Organization for Standardization, ISO/IEC 18028-3:2005-12-05, 2005, 3.8**
Other Source (Glossary or specific definition listed in document)

**- International Organization for Standardization, ISO/IEC 27000:2014, 2.36**
Other Source (Glossary or specific definition listed in document)

**- International Organization for Standardization, ISO/IEC 27035:2011-09-01, 3.4**
Other Source (Glossary or specific definition listed in document)

## Information Technologies Security Incident

An information technologies security incident (hereinafter – security incident) is a harmful event or offence, as a result of which the integrity, availability or confidentiality of information technologies is endangered.

**- Latvia, Law on Security of Information Technologies 2012, p. 3**
State > OSCE (Glossary or specific definition listed in document)

## Security Incident*

“ISO 17799 mentions incident, security incident and information security incident.
Only the term "security incident" is defined as a "security breach, threat, weakness and malfunction that might have an impact on the security of organizational assets". Nowhere are the terms "incident" and "information security incident" explained. In this Recommendation, it is assumed that an incident is less severe than a security incident and that an information security incident is a particular type of security incident.”
**- International Telecommunication Union, ITU-T, Rec. E.409, 2004, 1.2**
Intergovernmental Organization (Glossary or specific definition listed in document)

Any adverse event whereby some aspect of security could be threatened. [in force]
**- International Telecommunication Union, ITU-T, Rec. E.409, 2004, 1.2.3**
Intergovernmental Organization (Glossary or specific definition listed in document)

1. (I) A security event that involves a security violation.[9] (See: CERT, security event, security intrusion, security violation.)
Tutorial: In other words, a security event in which the system's security policy is disobeyed or otherwise breached.
2. (D) "Any adverse event [that] compromises some aspect of computer or network security."
Deprecated Definition: IDOCs SHOULD NOT use definition 2 because (a) a security incident may occur without actually being harmful (i.e., adverse) and because (b) this Glossary defines "compromise" more narrowly in relation to unauthorized access.
3. (D) "A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices."
Deprecated Definition: IDOCs SHOULD NOT use definition 3 because it mixes concepts in way that does not agree with common usage; a security incident is commonly thought of as involving a realization of a threat (see: threat action), not just a threat.
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

[9] An act or event that disobeys or otherwise breaches security policy. (See: compromise, penetration, security incident.)

# CRITICAL INFRASTRUCTURE

## Critical*

Qualitative description used to emphasize the importance of a resource, process or function that must be available and operational constantly or available and operational at the earliest possible time after an incident, emergency or disaster has occurred.
**- International Organization for Standardization, ISO/IEC 27031:2011-03-01, 2011, 3.5**
Other Source (Glossary or specific definition listed in document)

1. (I) /system resource/ A condition of a system resource such that denial of access to, or lack of availability of, that resource would jeopardize a system user's ability to perform a primary function or would result in other serious consequences, such as human injury or loss of life. (See: availability, precedence. Compare: sensitive.)
2. (N) /extension/ An indication that an application is not permitted to ignore an extension.
Tutorial: Each extension of an X.509 certificate or CRL is flagged as either "critical" or "non-critical". In a certificate, if a computer program does not recognize an extension's type (i.e., does not implement its semantics), then if the extension is critical, the program is required to treat the certificate as invalid; but if the extension is non-critical, the program is permitted to ignore the extension.
In a CRL, if a program does not recognize a critical extension that is associated with a specific certificate, the program is required to assume that the listed certificate has been revoked and is no longer valid, and then take whatever action is required by local policy.
When a program does not recognize a critical extension that is associated with the CRL as a whole, the program is required to assume that all listed certificates have been revoked and are no longer valid. However, since failing to process the extension may mean that the list has not been completed, the program cannot assume that other certificates are valid, and the program needs to take whatever action is therefore required by local policy.
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Critical ICT Infrastructure

Critical ICT infrastructure is defined as critical infrastructure for electronic communications. See also ICT infrastructure.
**- Norway, Cyber Security Strategy for Norway, 2012, p. 28**
State > OSCE (Glossary or specific definition listed in document)

## Critical Information Infrastructure

Critical information infrastructure (CII) may refer to any IT systems which support key assets and services within the national infrastructure.
**- United Kingdom, Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK, 2011, p. 2**
State > P5 (In Paragraph)

Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information systems within the field of cybersecurity.
**- Czech Republic, Draft Act on Cyber Security, 2014, p. 2**
State > OSCE (Glossary or specific definition listed in document)

Critical information infrastructure shall mean an electronic communications network, information system or a group of information systems where an incident that occurs causes or may cause grave damage to national security, national economy or social well-being.
**- Lithuania, Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019, 2011, p. 2**
State > OSCE (Glossary or specific definition listed in document)

(I) Those systems that are so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety.
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Critical Infrastructure

As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
**- United States of America, Executive Order: Improving Critical Infrastructure Cybersecurity, 2013, p. 1**
State > P5 (Glossary or specific definition listed in document)

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
**- United States of America, Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2014, p. 37**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 51**
State > P5 (Glossary or specific definition listed in document)

The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Although governments administer only a minority of the Nation's critical infrastructure computer systems, governments at all levels perform essential services that rely on each of the critical infrastructure sectors, which are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.
**- United States of America, The National Strategy to Secure Cyberspace, 2003, p. 4**
State > P5 (In paragraph)

Translation: It is the set of computers, computer systems, communication networks, data and information, the destruction of or interference with which may weaken or impact the economic security, public health, or combination thereof, in a nation.[xxiv]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 39**
State > UNGGE4 (Glossary or specific definition listed in document)

Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences. At federal level, the following areas have been identified: Energy, information technology and telecommunication, transport, health, wather, food, finance and insurance sector, state and administration, media and culture.
**- Germany, Cyber Security Strategy for Germany, 2011, p. 15**
State > UNGGE4 (Glossary or specific definition listed in document)

Critical infrastructures are formed by business entities providing highly irreplaceable services and are essential for people's social lives and economic activities. If its function is suspended, reduced or unavailable, peoples social lives and economic activities will be greatly disrupted, and the same below.
**- Japan, The First National Strategy on Information Security, 2006, p. 11**
State > UNGGE4 (Footnote Definition)

Critical infrastructures are those infrastructures or parts thereof which are of crucial importance for ensuring important social functions. Their failure or destruction has severe effects on the health, security or the economic and social wellbeing of the population or the functioning of governmental institutions. Critical infrastructure is often abbreviated as CI (Critical Infrastructure) even in the German-language area. CIP has become the abbreviation commonly used at international and national level, referring to Critical Infrastructure Protection, while CIIP stands for Critical Information Infrastructure Protection.
**- Austria, Austrian Cyber Security Strategy, 2013, p. 20**
State > OSCE (Glossary or specific definition listed in document)

Information infrastructure is a key component of Canada's critical infrastructure, which includes the following sectors: energy and utilities, communications and information technology, finance, health care, food, water, transportation, Government and manufacturing. The challenges of securing the information infrastructure are the same across all sectors, of which up to 90 per cent is estimated to be owned and operated privately.
**- Canada, Submission to the United Nations General Assembly Resolution A/60/95/Add.1, p. 4**
State > OSCE (In paragraph)

Critical infrastructure is an asset or system within the EU which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption may have a significant negative impact for the security of the EU and the well-being of its citizens.
**- Italy, 2013 National Strategic Framework for cyberspace security, 2013, p. 42**
State > OSCE (Glossary or specific definition listed in document)

Society's functional ability is highly dependent on a number of physical and technical infrastructures. In the event of a failure in these infrastructures, society will be unable to maintain the supply of goods and services on which the population depends (cf. critical societal functions). These infrastructures can be described as critical to society.
**- Norway, Cyber Security Strategy for Norway, 2012, p. 28**
State > OSCE (Glossary or specific definition listed in document)

Critical infrastructure refers to infrastructure whose disruption, failure or destruction would have serious implications for society, the private sector and the state. It includes, for example, control and switchgear for energy supply or telecommunications. An inventory of critical infrastructure will be compiled by the national strategy for the protection of critical infrastructure.
**- Switzerland, National Strategy for the Protection of Switzerland Against Cyber Risks, 2012, p. 6**
State > OSCE (Footnote Definition)

The infrastructures which host the information systems that can cause: loss of lives; Large scale economic damages; Security vulnerabilities and disturbance of public order at national level when the confidentiality, integrity or accessibility of the information they process is compromised.
**- Turkey, National Cyber Security Strategy and 2013-2014 Action Plan, 2013, p. 9**
State > OSCE (Glossary or specific definition listed in document)

Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia's ability to ensure national security.
**- Australia, Cyber Security Strategy, 2009, 20**
State > Other (Glossary or specific definition listed in document)

System and assets, whether physical or virtual, so vital to KSA that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
**- Saudi Arabia, Developing National Information Security Strategy for the Kingdom of Saudi Arabia, 2013, p. A-1**
State > Other (Glossary or specific definition listed in document)

Physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment.
**- NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare, 2013, p. 258**
Other Source (Glossary or specific definition listed in document)

Organizations and facilities that are essential for the functioning of society and the economy as a whole
NOTE: A failure or malfunction of such organizations and facilities would result in sustained supply shortfalls, make a significant impact on public security and have other wide ranging impacts.
**- International Organization for Standardization, ISO/IEC TR 27019:2013, 3.3**
Other Source (Glossary or specific definition listed in document)

## Critical Infrastructure and Key Resources

The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2014, p. 61** (JP 3-27)
State > P5 (Glossary or specific definition listed in document)

## Critical National Infrastructure

A term used by governments to describe assets that are essential for the functioning of a society and economy (e.g. electricity generation, gas production, telecommunications, water supply etc.).
**- New Zealand, New Zealand's Cyber Security Strategy, 2011, p. 12**
State > Other (Glossary or specific definition listed in document)

## Cyber Infrastructure

The information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements: Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.
- **United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 58**
State > P5 (Glossary or specific definition listed in document)

Cyber Infrastructure is the aggregation of people, processes and systems that constitute cyberspace.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 18**
Other Source (Glossary or specific definition listed in document)

## Electronic Information Infrastructure*

A condition of an electronic information system in which its protection is closed, comprehensive, continuous and commensurate with risks in terms of the confidentiality, integrity and availability of the data managed in such electronic information system, as well as of the integrity and availability of the electronic information system elements.
**- Hungary, Annex 1 to Government Decision No. 1139/2013 National Cyber Security Strategy of Hungary, 2013, p. 2**
State > OSCE (Glossary or specific definition listed in document)

## Global Information Infrastructure*

A collection of networks, end user equipment, information, and human resources which can be used to access valuable information, communicate with each other, work, learn, receive entertainment from it, at any time and from any place, with affordable cost on a global scale.
**- International Telecommunication Union, ITU-T, Y.101, 2000, 33**
Intergovernmental Organization (Glossary or specific definition listed in document)

## ICT Infrastructure*

Electronic systems that process data or communicate with other equipment, on which a unit or organisation is dependent to function effectively.
**- Norway, Cyber Security Strategy for Norway, 2012, p. 28**
State > OSCE (Glossary or specific definition listed in document)

## Information Infrastructure

Translation: A set of technical means and systems of formation, creation, conversion, transmission, use, and storage of information.[xxv]
**- Russia, Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве), 2011**
State > P5 (Glossary or specific definition listed in document)

Translation: The totality of an infrastructure's IT componens is referred to as its information infrastructure.[xxvi]
**- Germany, Implementation Plan KRITIS, 2007**
State > UNGGE4 (Glossary or specific definition listed in document)

## National Critical Infrastructure and Key Assets

The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 249 (JP 3-28)**
State > P5 (Glossary or specific definition listed in document)

## Vital Structures

A State's facilities, systems and institutions, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, energy supply, credit and finance, communications, State administrative bodies, the defence system, law-enforcement agencies, strategic information resources, scientific establishments and scientific and technological developments, installations that pose heightened technological and environmental risks, and bodies for eliminating the consequences of natural disasters or other emergency situations).
**- Russia, Submission to the United Nations General Assembly Resolution A/54/213, p. 10**
State > P5 (Glossary or specific definition listed in document)

Vital structures — facilities, systems and institutions of a State, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, power supply, credit and finance, communications, State administrative bodies, defence system, law enforcement agencies, strategic information resources, scientific facilities and scientific and technological developments, installations entailing a high degree of technological or ecological risk, bodies for the mitigation of the effects of natural disasters or other emergencies).
**- Russia, Submission to the United Nations General Assembly Resolution A/55/140, p. 4**
State > P5 (Glossary or specific definition listed in document)

# WEAPON

## Cyber Weapon

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. It is a safe prediction that the use of cyberweaponry will shortly become ubiquitous.
**- Sommer and Brown For OECD/IFP Project on Future Global Shocks – Reducing Systemic Cybersecurity Risk, 2011, p. 6**
Other Source (In paragraph)

Software, firmware or hardware designed or applied to cause damage through the cyber domain.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 56**
Other Sources (Glossary or specific definition listed in document)

## Information Weapon

Means and methods used with a view to damaging another State's information resources, processes and systems; use of information to the detriment of a State's defence, administrative, political, social, economic or other vital systems, and the mass manipulation of a State's population with a view to destabilizing society and the State.
**- Russia, Submission to the United Nations General Assembly Resolution A/54/213, p. 10**
State > P5 (Glossary or specific definition listed in document)

Ways and means used for the purpose of damaging the information resources, processes and systems of a State, exerting an adverse influence, through information, on the defence, administrative, political, social, economic and other vital systems of a State, as well as the massive psychological manipulation of a population in order to destabilize society and the State.
**- Russia, Submission to the United Nations General Assembly Resolution A/55/140, p. 3**
State > P5 (Glossary or specific definition listed in document)

Translation: Information technology, tools, and methods used for the purpose of information warfare.[xxvii]
**- Russia, Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве), 2011**
State > P5 (Glossary or specific definition listed in document)

Information and telecommunication systems can become weapons when they are designed and/or used to inflict damage on a State's infrastructure. Examples include attacks on national networks with foreign software or from internal sources within the State itself that are planned or conceived abroad; radio or television broadcasts through unauthorized means or without the consent of the State attacked; and influencing the conduct of persons with a view to destabilizing societies, overthrowing governments or altering the political and social order of countries.
**- Cuba, Submission to the United Nations General Assembly Resolution A/56/164/Add.1, p. 4**
State > Other (In paragraph)

Information and telecommunication systems can become weapons when they are designed or used to cause harm to a State's infrastructure. For example, attacking national networks with foreign software or from sources within the State, but promoted or conceived from abroad; radio and television broadcasts intended to disrupt the social order and the institutional framework deriving from the Constitution of another State to which these signals are sent; activities intended to interfere with, damage or paralyse the broadcasting services of other States, etc.
**- Cuba, Submission to the United Nations General Assembly Resolution A/58/373, p. 5**
State > Other (In paragraph)

Information resources strategically developed or created for information warfare or to cause damage, confusion or disadvantage and with any other forms of malicious intent.
**- Philippines, Submission to the United Nations General Assembly Resolution A/56/164, p. 4**
State > Other (Glossary or specific definition listed in document)

## Use of the Internet as a Weapon

Use of the Internet as a weapon, i.e., its use as a means to launch attacks against critical infrastructure information systems or the infrastructure of the Internet itself.
**- Spain, Submission to the United Nations General Assembly Resolution A/64/129/Add.1, p. 10**
State > UNGGE4 (In paragraph)

# CRIME

## Cyber Crimes or Information Crimes

(i) Criminal acts involving elements of information security; (ii) acts of malicious intent directed at information resources (e.g. techno-vandalism, techno-trespass and superzapping); (iii) all unauthorized interference or unsanctioned penetration.
**- Philippines, Submission to the United Nations General Assembly Resolution A/56/164, p. 4**
State > Other (In paragraph)

## Cybercrime

Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime.
**- France, Information Systems Defence and Security: France's Strategy, 2011, p. 21**
State > P5 (Glossary or specific definition listed in document)

For the purposes of this study, we are using the term 'cyber crime' to mean the illegal activities undertaken by criminals for financial gain. Such activities exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the Government.
**- United Kingdom, The Cost of Cyber Crime, 2011, p. 1**
State > P5 (In Paragraph)

Translation: Illicit actions which are committed through the utilization of a computer service or good. (Ministry of Defense of Colombia)[xxviii]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 38**
State > UNGGE4 (Glossary or specific definition listed in document)

Translation: Criminal or abusive activities on computers or communication networks, either because the computer is used as the tool of the crime, or because the computer system (or data) is the objective of the crime. (Ministry of Defense of Colombia)[xxix]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 38**
State > UNGGE4 (Glossary or specific definition listed in document)

The majority of attacks against information systems and the data stored therein are crimes committed for financial gain. These crimes may manifest themselves in a disruption to a particular financial service or in a violation of the confidentiality, integrity or availability of financial data. Other forms of cyber crime include harassment, fraud, the distribution of illegal materials or the violation of intellectual property rights. To the criminal, the use of cyberspace for securing material profit might seem attractive because of the simplicity and remoteness with which such crimes can be committed. Other factors which lend to the appeal of cyber crime are: anonymity, deficiencies in international regulation of the use of cyberspace and the negligence of information system owners and end-users in ensuring the security of cyberspace.
**- Estonia, Cybersecurity Strategy, 2008**
State > UNGGE4 (In paragraph)

Translation: Cybercrime encompasses offenses
- that are directed against the Internet, data networks, information technology systems or their data,
- that are committed by means of information technology,"[xxx]
**- Germany, Federal Criminal Police Office – Federal Overview Cybercrime 2013, 2013**
State > UNGGE4 (Glossary or specific definition listed in document)

Translation: Criminal activity through which services or applications in cyberspace are being used to carry out crime or are targets of crime. In the process, cyberspace can be origin, target or the environment of the attack.[xxxi]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

Cyber crime comprises illegal attacks from cyber space on or through ICT systems, which are defined in penal or administrative laws. The term therefore covers all criminal offences committed with the aid of information technologies and communications networks and also encompasses Internet crime.
**- Austria, Austrian Cyber Security Strategy, 2013, p. 21**
State > OSCE (Glossary or specific definition listed in document)

Translation: Cybercrime is an offense abusing, in terms of medium, the automation and automated data and also being applicable to information systems or data stored on them.
**- Belgium, Cyber Security Strategy, 2012, p. 12**
State > OSCE (Glossary or specific definition listed in document)

These offences can be roughly divided into three categories:
(a) Universal, State and public offences, which represent a threat to national and public security (including calls to overthrow the existing order, attempts to devalue sovereignty or to undermine independence and national interests, terrorist propaganda, chauvinism, xenophobia, all forms of extremism, and discrimination on ethnic, racial, religious, gender and other grounds);
(b) Universal civil offences, which constitute a threat to individual rights and freedoms (including violations of individual rights and freedoms, the use of compromising material, the exertion of pressure on individuals, the discrediting of individuals, the dissemination of confidential information, the use of another person's Internet services, the forgery of documents and copyright infringement);
(c) Traditional offences, which threaten the foundations of morality and decency (including pornography, paedophilia, other forms of sexual perversion, drug addiction and alcoholism).
**- Kazakhstan, Submission to the United Nations General Assembly Resolution A/64/129, p. 4**
State > OSCE (Full passage)

An offence committed in cyberspace.
**- Poland, Cyberspace Protection Policy of the Republic of Poland, 2013, 5**
State > OSCE (Glossary or specific definition listed in document)

The Australian Government defines cyber crime as those computer offences under the Commonwealth Criminal Code Act 1995 (Part 10.7) which involve the unauthorised access to, modification or impairment of electronic communications.
**- Australia, Cyber Security Strategy, 2009, p. 23**
State > Other (In text box)

Information and communication technologies have been widely adopted in societies and are considered to be the foundations that support the current globalized world; however, this widespread usage, among other things, has exposed the information generated, published and stored using information and

communication technologies to a wide range of threats, known as cybercrime, that can have a serious impact on such areas as the confidentiality, integrity and availability of the information.
**- Ecuador, A66/152/Add.1, p. 5**
State > Other (In paragraph)

Any crime where information and communications technology is: 1. used as a tool in the commission of an offence; 2. the target of an offence; 3. a storage device in the commission of an offence.
**- New Zealand, New Zealand's Cyber Security Strategy, 2011, p. 12**
State > Other (Glossary or specific definition listed in document)

Cybercrime means cyber crimes as defined in chapter XIII of the ECT Act (no.25 of 2002).
**- South Africa, Notice of Intention to make South African National Cybersecurity Policy, 2010, p. 12**
State > Other (In paragraph)

Cyber-crime involving inter alia malware, viruses, identity theft and attacks on financial institutions.
**- South Africa, South African Defence Review 2012, 2012, p. 79**
State > Other (In paragraph)

Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).
**- European Union, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, p. 3**
Intergovernmental Organization (In paragraph)

Criminal activity where services or applications in the Cyberspace are used for or are the target of crime, or where the Cyberspace is the source, tool, target, or place of a crime.
**- International Organization for Standardization, ISO/IEC 27032:2012, 2012, 4.18**
Other Source (Glossary or specific definition listed in document)

Cyber crime is the use of cyberspace for criminal purposes as defined by national or international law.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 29**
Other Source (Glossary or specific definition listed in document)

Crime committed on or using a computer or computer network.
**- Oxford University, A Dictionary of Computing, 2008, p. 120**
Other Source (Dictionary)

## Information Crime

Translation: All actions under criminal law or other special law that present a social threat and the guilty actions are committed through or over cyber infrastructure.[xxxii]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 8**
State > OSCE (Glossary or specific definition listed in document)

## Internet Crime*

Criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime.
**- International Organization for Standardization, ISO/IEC 27032:2012, 2012, 4.30**
Other Source (Glossary or specific definition listed in document)

# ESPIONAGE

## Cyber Espionage

Cyber attacks have aimed to steal sensitive information and data from financial, government and utilities infrastructure targets. These attacks can target intellectual property or sensitive information about organisations or government.
**- United Kingdom, Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK, 2011, p. 2**
State > P5 (In Paragraph)

Cyber attacks directed against the confidentiality of an IT system, which are launched. or managed by foreign intelligence services, are called cyber espionage.
**- Germany, Cyber Security Strategy for Germany, 2011, p. 14-15**
State > UNGGE4 (Glossary or specific definition listed in document)

Cyber attacks directed against the confidentiality of an IT system are referred to as "cyber espionage", i.e. digital spying.
**- Austria, Cyber Security Strategy, 2013, p. 20**
State > OSCE (Glossary or specific definition listed in document)

Cyber espionage is defined as "the use of an agent in order to obtain information about plans or activities of foreign country or competitive company". It is not uncommon that companies or governments are faced with attempts of unauthorised access to their computer systems via Internet. Many countries use espionage tools to encourage their economic development based on advanced technologies of other nations. ICT present foundation of development and implementation of most other technologies both in civilian and military sectors, and thereupon they have become primary target of espionage.
**- Montenegro, National Cyber Security Strategy for Montenegro 2013-2017, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

Translation: Actions carried out in cyberspace with the purpose of obtaining unauthorized, confidential information in the interest of state or non state entities.[xxxiii]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 8**
State > OSCE (Glossary or specific definition listed in document)

Cyber-espionage involving inter alia the silent gathering of information.
**- South Africa, South African Defence Review 2012, 2012, p. 79**
State > Other (In paragraph)

"Cyber espionage" is defined narrowly as any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather_ information with the intention of communicating it to the opposing party. The act must occur in territory controlled by a party to the conflict.
**- NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare, 2013, p. 193**
Other Source (In paragraph)

A cyber operation to obtain unauthorized access to sensitive information through covert means.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 40**
Other Source (Glossary or specific definition listed in document)

The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.
**- The Oxford English Dictionary, 2014**
Other Source (Dictionary)

# SABOTAGE

## Cyber Sabotage

Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage.
**- Germany, Cyber Security Strategy for Germany, 2011, p. 15**
State > UNGGE4 (Glossary or specific definition listed in document)

Cyber attacks directed against the integrity and availability of an IT system are referred to as cyber sabotage.
**- Austria, Austrian Cyber Security Strategy, 2013, p. 20**
State > OSCE (Glossary or specific definition listed in document)

# TERRORISM

## Cyber Terrorism

Translation: The convergence of terrorism and cyberspace with the goal of unlawfully attacking computers, networks and information stored on them, including [inducing] violence against persons or property or, at least, generating fear. This includes murder, explosions, contamination of water or large economic losses, among other actions. (Dorothy Dennigal, Professor, Georgetown University)[xxxiv]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 39**
State > UNGGE4 (Glossary or specific definition listed in document)

Various forms of cyber terrorism: Hacking, DDoS attacks, denials of service, logic bombs, Trojan horses, Worm viruses, HERF guns etc.
**- South Korea, Defense White Paper 2012, 2012, p. 10**
State > UNGGE4 (In paragraph)

Cyber terrorism is defined as a politically motivated crime of state and / or non-state actors against computers, networks and the information stored therein. Its aim is to provoke a severe or long-term disruption of public life or to cause serious damage to economic activity with the intention of severely intimidating the population, of forcing public authorities or an international organisation to carry out, tolerate or omit an act or of profoundly unsettling or destroying the political, constitutional, economic or social foundations of a state or an international organisation. These acts constitute organised cyber sabotage (attacks) caused by political-fundamentalist groups or individual perpetrators; they are directed against states, organisations or enterprises.
- **Austria, Austrian Cyber Security Strategy, 2013, p. 21**
State > OSCE (In paragraph)

Terrorist networks also are moving to incorporate cyber operations into their strategic doctrines. Among many activities, they are using the Internet to support their recruitment, fundraising and propaganda activities.
Terrorists are aware of the potential for using the Western world's dependence on cyber systems as a vulnerability to be exploited. For example, there are now online resources providing advice to terrorists on how to defend their own websites while launching cyber attacks on their enemies. In addition, a number of terrorist groups, including Al-Qaeda, have expressed their intention to launch cyber attacks against Western states. Though experts doubt that terrorists currently have the ability to cause serious damage via cyber attacks, they recognize that this capacity will likely develop over time.
**- Canada, Canada's Cyber Security Strategy For A Stronger and More Prosperous Canada, 2010, p. 5**
State > OSCE (Full passage)

Ideologically motivated exploitations of systems' vulnerabilities with the intent of influencing a state or an international organization.
**- Italy, 2013 National Strategic Framework for Cyberspace Security, 2013, p. 13**
State > OSCE (Glossary or specific definition listed in document)

Cyber terrorism is a criminal act in cyberspace that aims to intimidate governments or their citizens, with the aim to achieve political goals. NIPC (National Infrastructure Protection Center) defines cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies".
**- Montenegro, National Cyber Security Strategy for Montenegro 2013-2017, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

An offence of a terrorist nature committed in cyberspace.
**- Poland, Cyberspace Protection Policy of the Republic of Poland, 2013, p. 5**
State > OSCE (Glossary or specific definition listed in document)

Translation: Malicious activities carried out in cyberspace by individuals, groups, or organizations motivated by political, ideological, or religious causes that may cause material damage or casualties, likely to cause panic or terror.[xxxv]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 8**
State > OSCE (Glossary or specific definition listed in document)

We define cyberterrorism as cyber-related terrorism and more specifically, for our purposes, as terrorist attacks on cyber infrastructure particularly on control systems for non-nuclear critical energy infrastructure.
**- OSCE, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, 2013, 16**
Intergovernmental Organization (In paragraph)

Cyber terrorism is the use of cyberspace for terrorist purposes as defined by national or international law.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 30**
Other Source (Glossary or specific definition listed in document)

The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.
**- The Oxford English Dictionary, 2014**
Other Source (Dictionary)

## Information Terrorism

Terroristic acts in the context of information security.
**- Philippines, Submission to the United Nations General Assembly Resolution A/56/164, p. 4**
State > Other (Glossary or specific definition listed in document)

Terrorist activities that use information and communication technologies, including networks.
**- SCO, International Code of Conduct for Information Security, 2011, p. 4**
Intergovernmental Organization (In paragraph)

## International Information Terrorism

The use of telecommunications and information systems and resources and exerting influence on such systems or resources in the international information area for terrorist purposes.
**- Russia, Submission to the United Nations General Assembly Resolution A/55/140, p. 4**
State > P5 (Glossary or specific definition listed in document)

## Use of the Internet for Terrorist Purposes

Our Criminal Code criminalizes, suppresses and punishes use of the Internet for terrorist purposes. Article 289 states "Any person using the Internet to provide training for the commission of terrorist acts or to recruit others to commit such acts shall be punished by imprisonment for five to ten years."
**- Panama, Submission to the United Nations General Assembly Resolution A/65/154, p. 9**
State > Other (In paragraph)

# WAR & WARFARE

## Cyber War

Cyber war refers to acts of war in and around virtual space with means which are predominantly associated with information technology. In a broader sense, this implies the support of military campaigns in traditional operational spaces – i.e. ground, sea, air and outer space – through measures taken in the virtual space. In general, the term also refers to high-tech warfare in the information age based on the extensive computerisation, electronisation and networking of almost all military sectors and issues.
- **Austria, Austrian Cyber Security Strategy, 2013, p. 22**
State > OSCE (Glossary or specific definition listed in document)

Translation: The use of cyber capabilities of a sufficient scale for a specific period and at high speed, in order to achieve certain objectives or effects in or through cyberspace; such actions are considered a threat to the national interests of state goals.[xxxvi]
**- Belgium, Cyber Security Strategy, 2012, p. 12**
State > OSCE (Glossary or specific definition listed in document)

Cyber war is unspecified and controversial term that has no official or generally accepted definition. More than 30 countries have accepted the doctrine and announced development of a special programme of cyber war offensive mechanisms.
**- Montenegro, National Cyber Security Strategy for Montenegro 2013-2017, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

Cyber War is an escalated state of cyber conflict between or among states in which cyber attacks are carried out by state actors against cyber infrastructure as part of a military campaign
(i) Declared: that is formally declared by an authority of one of the parties,
(ii) De Facto: with the absence of a declaration.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 32**
Other Source (Glossary or specific definition listed in document)

A true cyberwar is an event with the characteristics of conventional war but fought exclusively in cyberspace.
**- Sommer and Brown For OECD/IFP Project on Future Global Shocks – Reducing Systemic Cybersecurity Risk, 2011, p. 6**
Other Source (In paragraph)

It is much easier to define "cyberwar" as the tests are the same as for any conventional "kinetic" war. Some of the key international treaties include the 1899 and 1907 Hague Conventions, 1945 UN Charter, 1948 UN Genocide Convention and the 1980 UN Convention on Excessively Injurious Conventional Weapons. In essence, to decide whether an act amounts to cyberwar one applies a test to see whether it was "equivalent" to a conventional hostile attack and looks to scope, intensity and duration. There is also a distinction between acts aimed at military and civilian targets.
**- Sommer and Brown For OECD/IFP Project on Future Global Shocks – Reducing Systemic Cybersecurity Risk, 2011, p. 12**
Other Source (Full passage)

The use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems.
**- The Oxford English Dictionary, 2014**
Other Source (Dictionary)

## Cyber Warfare

Activities and operations carried out in the cyber domain with the purpose of achieving an operational advantage of military significance.
**- Italy, 2013 National Strategic Framework for cyberspace security, 2013, p. 13**
State > OSCE (Glossary or specific definition listed in document)

Cyber-warfare involving inter alia offensive information operations.
**- South Africa, South African Defence Review 2012, 2012, p. 79**
State > Other (In paragraph)

Cyber Warfare is cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 43**
Other Source (Glossary or specific definition listed in document)

## Information War

Confrontation between States in the information field, with a view to damaging information systems, processes and resources and vital structures, and undermining another State's political and social systems, as well as the mass psychological manipulation of a State's population and the destabilization of society.
**- Russia, Submission to the United Nations General Assembly Resolution A/54/213, 10**
State > P5 (Glossary or specific definition listed in document)

Confrontation between States in the information area for the purpose of damaging information systems, processes and resources and vital structures, undermining political, economic and social systems as well as the massive psychological manipulation of a population in order to destabilize society and the State.
**- Russia, Submission to the United Nations General Assembly Resolution A/55/140, p. 3**
State > P5 (Glossary or specific definition listed in document)

Translation: The confrontation between two or more states in the information space with the purpose of causing harm to information systems, processes and resources and other critical structures, undermining the political, economic and social systems, massive psychological treatment of the population to destabilize society and the state, as well as forcing the state to take decisions in the interests of the opposing side.[xxxvii]
**- Russia, Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве), 2011**
State > P5 (Glossary or specific definition listed in document)

Information War is an escalated state of information conflict between or among states in which information operations are carried out by state actors for politico-military purposes.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 35**
Other Source (Glossary or specific definition listed in document)

## Information Warfare

(i) Actions aimed at achieving information superiority by executing measures to exploit, corrupt, destroy, destabilize or damage the enemy's information and its functions; (ii) actions taken to protect one's information resources and telecommunication systems; (iii) acts of exploiting one's information resources and telecommunications systems to achieve goals and interests, for example, cyber warfare (information warfare in the defence and military context) or "Internet war" (information warfare in the larger societal context).
**- Philippines, Submission to the United Nations General Assembly Resolution A/56/164, p. 4**
State > Other (Glossary or specific definition listed in document)

Although the terms cyber-warfare, cyber-defence or cyber-attack are often used in everyday speak, the broad military concept used in this goal is Information Warfare, a term which covers a broad range of operations to be carried out within the Information Sphere (commonly also known as the InfoSphere).
**- South Africa, South African Defence Review 2012, 2012, p. 146**
State > Other (In paragraph)

# OTHERS

## Attack*

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 11**
State > P5 (Glossary or specific definition listed in document)

Translation: An attack is an intentional form of threat, namely an undesirable or unauthorized action with the objective to gain advantages or harm a third party respectively. Attackers can also act on behalf of third parties that want to gain advantages.[xxxviii]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly. [in force]
**- International Telecommunication Union, ITU-T, Rec. H.235.0 (01/2014), 2014, 3.2.2**
Intergovernmental Organization (Glossary or specific definition listed in document)

An attack may either be a known attack or an unknown attack. The known attack means that the pattern or packet for attack is opened. Although the pattern or packet for attack is not opened for the unknown attack, it refers to the behaviour related to worsening network situation. [in force]
**- International Telecommunication Union, ITU-T X.1036 (11/2007), 2007**
Intergovernmental Organization (Glossary or specific definition listed in document)

Attempts to destroy, expose, alter, or disable an Information System and/or information within it or otherwise breach the security policy.
**- International Organization for Standardization, ISO/IEC 18043:2006, 2006, 2.1**
Other Source (Glossary or specific definition listed in document)

Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
**- International Organization for Standardization, ISO/IEC 27032:2012, 2012, 4.8**
Other Source (Glossary or specific definition listed in document)

1. (I) An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat. (See: penetration, violation, vulnerability.)
2. (I) A method or technique used in an assault (e.g. masquerade). (See: blind attack, distributed attack.)
Tutorial: Attacks can be characterized according to intent:

- An "active attack" attempts to alter system resources or affect their operation.
- A "passive attack" attempts to learn or make use of information from a system but does not affect system resources of that system. (See: wiretapping.) The object of a passive attack might be to obtain data that is needed for an off-line attack.

- An "off-line attack" is one in which the attacker obtains data from the target system and then analyzes the data on a different system of the attacker's own choosing, possibly in preparation for a second stage of attack on the target.

Attacks can be characterized according to point of initiation:

- An "inside attack" is one that is initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by the party that granted the authorization.
- An "outside attack" is initiated from outside the security perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Attacks can be characterized according to method of delivery:

- In a "direct attack", the attacker addresses attacking packets to the intended victim(s).
- In an "indirect attack", the attacker addresses packets to a third party, and the packets either have the address(es) of the intended victim(s) as their source address(es) or indicate the intended victim(s) in some other way. The third party responds by sending one or more attacking packets to the intended victims. The attacker can use third parties as attack amplifiers by providing a broadcast address as the victim address (e.g., "smurf attack"). (See: reflector attack. Compare: reflection attack, replay attack.)

**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Attacker*

Any person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources.
**- International Organization for Standardization, ISO/IEC 18028-3:2005, 2005, 3.2**
Other Source (Glossary or specific definition listed in document)
**- International Organization for Standardization, ISO/IEC 27033-1:2009, 2009, 3.3**
Other Source (Glossary or specific definition listed in document)

Person seeking to exploit potential vulnerabilities of a biometric system.
**- International Organization for Standardization, ISO/IEC 19792:2009-08-01, 2009, 4.1.2**
Other Source (Glossary or specific definition listed in document)

## Computer Network Attack

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 73 (JP 3-13)**
State > P5 (Dictionary)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 41**
State > P5 (Glossary or specific definition listed in document)

Activities that are conducted in and through the cyberspace in order to manipulate, obstruct, deny, downgrade or destroy information stored in the ICT networks or in the computer systems, or the ICT networks or in the computer systems themselves.
**- Italy, National Strategic Framework for Cyberspace Security, 2013, p. 41**
State > OSCE (Glossary or specific definition listed in document)

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. Note: A computer network attack is a type of cyber attack.
**- NATO, NATO AAP-06, 2014, 2-C-11**
Intergovernmental Organization (Glossary or specific definition listed in document)

## Computer Network Defense

Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 73 (JP 6-0)**
State > P5 (Glossary or specific definition listed in document)

The actions taken to defend against unauthorized activity within computer networks.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 41**
State > P5 (Glossary or specific definition listed in document)

Actions taken by using computer networks for protecting, monitoring, analyzing, detecting, and hindering non-authorized activities carried out against computer networks and IT systems.
**- Italy, National Strategic Framework for Cyberspace Security, 2013, p. 41**
State > OSCE (Glossary or specific definition listed in document)

## Computer Network Exploitation

Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
**- United States of America, Information Operations Joint Publication 3-13, 2006, GL-6**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 41**
State > P5 (Glossary or specific definition listed in document)

Operations carried out in cyberspace in order to extract information from targeted ICT networks or computer systems. They are intelligence gathering activities, or actions preparing the execution of a cyber attack.
**- Italy, National Strategic Framework for Cyberspace Security, 2013, p. 41**
State > OSCE (Glossary or specific definition listed in document)

## Computer Network Operations

Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 73 (JP 3-13)**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 41**
State > P5 (Glossary or specific definition listed in document)

Like other parts of modern society, the Danish Armed Forces will become increasingly vulnerable to, among other things, hacker attacks on their information and communication infrastructure. Likewise, the use of cyberspace in general is rapidly gaining increasing importance in connection with military operations. Cyberspace has, in other words, become a battlespace. This development places increasing demands on the ability of Danish Armed Forces to take defensive and offensive measures in cyberspace.
**- Denmark, Danish Defence Agreement 2010-2014, 2009, p. 11**
State > OSCE (In paragraph)

This term generally encompasses Computer Network Attack (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE).
**- Italy, National Strategic Framework for Cyberspace Security, 2013, p. 41**
State > OSCE (Glossary or specific definition listed in document)

Translation: The complex process of planning, coordination, synchronization, harmonization, and development of action in cyberspace to protect, control, and use computer networks to obtain information superiority, while neutralizing enemy capabilities.[xxxix]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

## Cyber Attack

The term cyber attack can refer to anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as: gaining unauthorised access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems).
**- United Kingdom, Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK, 2011, p. 1**
State > P5 (In Paragraph)

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
**- United States of America, CNSS National Information Assurance Glossary, 2010, p. 22**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 57**
State > P5 (Glossary or specific definition listed in document)

Translation: Organized and/or premeditated misconduct of one or more individuals to cause damage to a computer system problems through action in cyberspace. (Ministry of Defense of Colombia)[xl]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 38**
State > UNGGE4 (Glossary or specific definition listed in document)

A cyber attack is 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 foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage.
**- Germany, Cyber Security Strategy for Germany, 2011, p. 14-15**
State > UNGGE4 (Glossary or specific definition listed in document)

Translation: Attacks carried out in cyberspace through tools, services, or applications in cyberspace; in the process, cyberspace can be origin, target or the environment of the attack.[xli]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

The term "cyber attack" refers to an attack through IT in cyber space, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally.
**- Austria, Austrian Cyber Security Strategy, 2013, p. 20**
State > OSCE (Glossary or specific definition listed in document)

Cyber attacks include the unintentional or unauthorised access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.
**- Canada, Canada's Cyber Security Strategy For A Stronger and More Prosperous Canada, 2010, p. 3**
State > OSCE (Glossary or specific definition listed in document)

The growing dependence on information and communication technologies increases the vulnerability of the state and its citizens to cyber attacks. Such attacks may be a new type of warfare, or may have a criminal, economic, or terroristic motive and be launched to destabilize the society. Leaks of strategic information and intrusions of ICTs of government agencies or strategic enterprises and companies providing essential functions of the state may endanger strategic interests of the Czech Republic. There are many examples showing how fast and diversified developments in the field of cyber security are. Attacks against ICT structures are increasingly sophisticated and more comprehensive. They make use of many different methods and are aimed against various targets. Their nature and motives of the attackers also change. Well-organized attacks are more and more often aimed at elements of critical infrastructure (hereinafter "CI"), which are vital for the functioning of the state. As ICTs have found their way into many important areas of everyday life, they themselves have become a critical infrastructure element.
**- Czech Republic, Cyber Security Strategy of the Czech Republic for the 2011-2015 Period, 2011, p. 4**
State > OSCE (Full passage)

Translation: Hostile action deployed to affect the cyberspace and cybersecurity.[xlii]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

Cyber attacks are carried out on computers, networks and data. They are aimed at disrupting the integrity of the data or the functioning of the infrastructure and restricting or interrupting their availability. They also seek to compromise the confidentiality or authenticity of information by means of unauthorised reading, deletion or modification of data, connections or server services are overloaded, information channels spied upon or surveillance and processing systems are manipulated in a targeted manner.
**- Switzerland, National Strategy for the Protection of Switzerland Against Cyber Risks, 2012, p. 9**
State > OSCE (Full passage)

An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission.
**- New Zealand, New Zealand's Cyber Security Strategy, 2011, p. 12**
State > Other (Glossary or specific definition listed in document)

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.
**- NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare, 2013, p. 106**
Other Source (Glossary or specific definition listed in document)

Cyber Attack is an offensive use of a cyber weapon intended to harm a designated target.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 44**
Other Source (Glossary or specific definition listed in document)

An attempt by hackers to damage or destroy a computer network or system.
**- The Oxford English Dictionary, 2014**
Other Source (Dictionary)

## Cyber Conflict

Cyber Conflict is a tense situation between and/or among nation states and/or organized groups where unwelcome cyber attacks result in retaliation.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 31**
Other Source (Glossary or specific definition listed in document)

## Cyber Defense

The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical.
**- France, Information Systems Defence and Security: France's Strategy, 2011, p.21**
State > P5 (Glossary or specific definition listed in document)

Translation: State capacity to prevent and counter any threat or incident that is cybernetic in nature which affects national sovereignty.[xliii]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 38**
State > UNGGE4 (Glossary or specific definition listed in document)

The term "cyber defence" refers to all measures to defend cyber space with military and appropriate means for achieving military-strategic goals. Cyber defence is an integrated system, comprising the implementation of all measures relating to ICT and information security, the capabilities of milCERT and CNO (Computer Network Operations) as well as the support of the physical capabilities of the army.
**- Austria, Austrian Cyber Security Strategy, 2013, p. 21**
State > OSCE (In paragraph)

Translation: Actions in cyberspace to protect, monitor, analyze, detect, counter aggression, and ensure appropriate response against specific cyber threats to national defense infrastructure.[xliv]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 7**
State > OSCE (Glossary or specific definition listed in document)

(Active Cyber Defence) A proactive measure for detecting or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber counter-operation against the source.
**- NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare, 2013, p. 257**
Other Source (Glossary or specific definition listed in document)

Cyber Defense is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attacks.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 47**
Other Source (Glossary or specific definition listed in document)

## Cyber Infrastructure Resilience

Translation: The ability of cyber infrastructure to withstand components of a cyber incident or attack and return to normality.[xlv]
**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 8**
State > OSCE (Glossary or specific definition listed in document)

## Cyber Operations

In the NICE Workforce Framework, cybersecurity work where a person: Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid (GIG).
**- United states of America, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 2010, p. 6**
State > P5 (Glossary or specific definition listed in document)

The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.
**- NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on International Law Applicable to Cyber Warfare, 2013, p. 258**
Other Source (Glossary or specific definition listed in document)

Organized activities in cyberspace to gather, prepare, disseminate, restrict or process information to achieve a goal.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 41**
Other Source (Glossary or specific definition listed in document)

## Cyber Threat*

Threats in cyberspace are difficult to define as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public and private interests and actors. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated. It requires high-level training, an advanced legal framework, effective organisational co-operation and the allocation of considerable resources.

Threats in cyberspace can be classified in many ways. One of the most common is a threefold classification based on motivational factors: cyber crime, cyber terrorism and cyber warfare. However, as advanced technologies and attack methods make it difficult to define with any certitude or clarity the motives impulsing an attack, threats can also be classified on the basis of methods employed and on the extent of damage inflicted. The damage may be substantial owing to the high degree of interaction between computer networks and also the interdependence of services related to the information infrastructure. For instance, an attack against the server of one service provider might also cause disruption to the information systems of an unrelated agency, which may be part of the critical infrastructure, using the services of that very same provider. It should be stressed that any abuse of cyberspace for whatever purpose, from foolish or mischievous computer hacking to organised attacks against the critical infrastructure of a country, is harmful to society.

**- Estonia, Cybersecurity Strategy, 2008**

State > UNGGE4 (In paragraph)

Translation: (Realistic) possibility of an undesired incident consisting of harming a technical system, an individual, or an organization.[xlvi]

**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**

State > UNGGE4 (Glossary or specific definition listed in document)

Cyber threat means the possibility of action or an incident in the cyber domain which, when materialised, jeopardises some operation dependent on the cyber world.
Note: Cyber threats are information threats which, when materialised, jeopardise the correct or intended functioning of the information system.

**- Finland, Finland's Cyber Security Strategy, 2013, p. 13**

State > OSCE (Glossary or specific definition listed in document)

As dependency of Georgia's critical infrastructure on information technologies increases, challenges related to the protection of Georgian cyberspace are growing. During the 2008 Russian-Georgian war, the Russian Federation conducted large-scale cyber-attacks, in parallel with the ground, air, and naval attacks. These attacks showed that the protection of cyberspace is as important for national security as land, maritime, and air defenses.

**- Georgia, National Security Concept of Georgia, 2011, p. 8**

State > OSCE (Glossary or specific definition listed in document)

The complex of malicious conducts that can be exercised in and throughout cyberspace, or against cyberspace and its fundamental elements.

**- Italy, 2013 National Strategic Framework for cyberspace security, 2013, p. 12**

State > OSCE (Glossary or specific definition listed in document)

Translation: Circumstance or event that constitutes a potential threat to cyber security.[xlvii]

**- Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013, p. 7**

State > OSCE (Glossary or specific definition listed in document)

A danger, whether communicated or sensed, that can exercise a cyber vulnerability.

**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 38**

Other Sources (Glossary or specific definition listed in document)

The possibility of a malicious attempt to damage or disrupt a computer network or system.

**- The Oxford English Dictionary, 2014**

Other Source (Dictionary)

## Cyberspace Operations

The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 63 (JP 3-0)**
State > P5 (Glossary or specific definition listed in document)

## Exploit*

A technique to breach the security of a network or information system in violation of security policy.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Translation: An exploit (English to exploit "ausnutzen") is a systematic possibility to exploit vulnerabilities that were ignored during a program's development. In the process, security vulnerabilities and malfunctions of programs (or entire systems) are used with the help of a sequence of instructions, mostly to gain access to resources or to impair systems.[xlviii]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

Defined way to breach the security of an Information System through vulnerability.
**- International Organization for Standardization, ISO/IEC 18043:2006-06-15, 2006, 2.8**
Other Source (Glossary or specific definition listed in document)

## Hacker*

An unauthorized user who attempts to or gains access to an information system.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 83**
State > P5 (Glossary or specific definition listed in document)

Translation: A hacker accessing or surfing in an information system knowing that he or she does not have authorization.[xlix]
**- Belgium, Cyber Security Strategy, 2012, p. 12**
State > OSCE (Glossary or specific definition listed in document)

1. (I) Someone with a strong interest in computers, who enjoys learning about them, programming them, and experimenting and otherwise working with them. (See: hack. Compare: adversary, cracker, intruder.) Usage: This first definition is the original meaning of the term (circa 1960); it then had a neutral or positive connotation of "someone who figures things out and makes something cool happen".
2. (O) "An individual who spends an inordinate amount of time working on computer systems for other than professional purposes."
3. (D) Synonym for "cracker".

Deprecated Usage: Today, the term is frequently (mis)used
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

1. A person who attempts to breach the security of a computer system by access from a remote point especially by guessing or otherwise obtaining a password. The motive may be merely personal satisfaction, for example by endeavoring to access a system in another country, but it may occasionally have a sinister intent. 2. Originally, a person who had an instinctive knowledge enabling him or her to develop software apparently by trial and error.
**- Oxford University, A Dictionary of Computing, 2004, p. 235**
Other Source (Dictionary)

## Hacking*

Translation: Intended access to a computer system without required authorization by the user or owner.[1]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

The term used to describe malicious acts of a wide ranging nature such as overcoming access controls, denial of service, theft of information or installation of malware.
**- International Telecommunication Union, ITU-T, Rec. E.800 (09/2008), 2008, 3.1.3.11**
Intergovernmental Organization (Glossary or specific definition listed in document)

Intentionally accessing a computer system without the authorization of the user or the owner.
**- International Organization for Standardization, ISO/IEC 27032:2012-07-15, 2012, 4.25**
Other Source (Glossary or specific definition listed in document)

Unauthorized access to computer material.
**- Oxford University, A Dictionary of Computing, 2004, p. 235**
Other Source (Dictionary)

## Hacktivism*

Translation: ”Hacking“ with a political or social purpose[li]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

Hacking for a politically or socially motivated purpose.
**- International Organization for Standardization, ISO/IEC 27032:2012-07-15, 2012, 4.26**
Other Source (Glossary or specific definition listed in document)

## Information Assurance

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
**- United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 175 (JP 3-13)**
State > P5 (Dictionary)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 93**
State > P5 (Glossary or specific definition listed in document)
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Technical and managerial measures designed to ensure the confidentiality, integrity, availability, authenticity, possession or control, and utility of information and information systems.
**- Jordan, National Information Assurance and Cyber Security Strategy, 2012, p. 5**
State > Other (Glossary or specific definition listed in document)

## Information Operations

The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making process, information, and information systems while protecting our own.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 94**
State > P5 (Glossary or specific definition listed in document)

Information Operations include coordinated actions to influence enemy's decision-making process, affecting his information, information processes and systems, while protecting own. It is integrated employment of electronic warfare, psychological operaitons, military deception, operations security and kinetic military measures.
**- Lithuania, Lithuanian Military Doctrine, 2010, p. 56**
State > OSCE (Glossary or specific definition listed in document)

Organized activities to gather, prepare, disseminate, restrict or process information to achieve a goal.
**- EWI/IISI, Critical Terminology Foundations 2, 2011, p. 34**
Other Source (Glossary or specific definition listed in document)

## Information Threat*

Translation: The appearance of a potential or current situation where an actor has the capacity to generate a cyber attack against the population, territory and political organization of the state.[lii]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 38**
State > UNGGE4 (Glossary or specific definition listed in document)

## Intruder*

Individual who is conducting, or has conducted, an intrusion or attack against a victim's host, site, network, or organization.
**- International Organization for Standardization, ISO/IEC 18043:2006-06-15, 2006, 2.13**
Other Source (Glossary or specific definition listed in document)

An entity that gains or attempts to gain access to a system or system resource without having authorization to do so. (See: intrusion. Compare: adversary, cracker, hacker.)
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Intrusion*

An unauthorized act of bypassing the security mechanisms of a network or information system.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 104**
State > P5 (Glossary or specific definition listed in document)

Unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system.
**- International Organization for Standardization, ISO/IEC 27033-1:2009, 2009, 3.17**
Other Source (Glossary or specific definition listed in document)

1. (I) A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so. (See: IDS.)
2. (I) A type of threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. (See: unauthorized disclosure.)
Usage: This type of threat action includes the following subtypes:
- "Trespass": Gaining physical access to sensitive data by circumventing a system's protections.
- "Penetration": Gaining logical access to sensitive data by circumventing a system's protections.
- "Reverse engineering": Acquiring sensitive data by disassembling and analyzing the design of a system component.

- "Cryptanalysis": Transforming encrypted data into plain text without having prior knowledge of encryption parameters or processes. (See: main entry for "cryptanalysis".)
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Malware*

Software that compromises the operation of a system by performing an unauthorized function or process.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 93**
State > P5 (Glossary or specific definition listed in document)

Translation: Computer programs that are developed and used to carry out functions that are undesired by the user and potentially harmful (malicious software) Example: viruses, Trojans, worms.[liii]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

Translation: Malicious software in the context of this law are programs and other information technology routines and processes with the objective to use or delete data without authorization or with the objective to interfere with other information technology activity without authorization.[liv]
**- Germany, Law to Strengthen the Security of Federal Information Technology, 2009**
State > UNGGE4 (Glossary or specific definition listed in the text)

"Malicious software" shall mean software specifically designed or modified to cause the unauthorized destruction, blocking modification or copying of information and the disruption of the functioning of a computer, computer system or related networks.
**- Commonwealth of Independent States, Agreement on cooperation among states in combating offences relating to computer information, 2001, p. 1**
Intergovernmental Organization (Glossary or specific definition listed in document)

A generic name for software which intentionally performs actions which can damage data or disrupt systems.
**- International Telecommunication Union, ITU-T, Rec.E.800, 2008, 3.1.3.10**
Other Source (Glossary or specific definition listed in document)

Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.
NOTE: Viruses and Trojan horses are examples of malware.
**- International Organization for Standardization, ISO/IEC 27033-1:2009, 2009, 3.22**
Other Source (Glossary or specific definition listed in document)

A contraction of "malicious software". (See: malicious logic.)[10]
Deprecated Term: IDOCs SHOULD NOT use this term; it is not listed in most dictionaries and could confuse international readers.
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

## Threat*

A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact(create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.
Extended Definition: Includes an individual or group of individuals, entity such as an organization or a nation), action, or occurrence.
**- United States of America, National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology**
State > P5 (Glossary or specific definition listed in document)

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
**- United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 198**
State > P5 (Glossary or specific definition listed in document)

Translation: Potential violation of the security.[lv]
**- Colombia, Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa), 2011, p. 38**
State > UNGGE4 (Glossary or specific definition listed in document)

Translation: A threat generally is a circumstance or event through which harm can occur. The harm refers to a specific value such as financial assets, knowledge, items, or health. Translated into the world of information technology, a threat is a circumstance or event that can threaten the availability, integrity, or confidentiality of information through which the owner of the information is harmed.[lvi]
**- Germany, Federal Office for Information Security (BSI): Glossary/Terminology**
State > UNGGE4 (Glossary or specific definition listed in document)

A potential cause of an unwanted incident, which may result in harm to a system or organization.
**- International Telecommunication Union, ITU-T X.1601 (01/2014), 2014**
Intergovernmental Organization (Glossary or specific definition listed in document)

The likelihood or frequency of a harmful event occurring. [in force]
**- International Telecommunication Union, ITU-T X.1521 (04/2011), 2011, 3.2.6**
Intergovernmental Organization (Glossary or specific definition listed in document)

A potential violation of security. [in force]
**- International Telecommunication Union, ITU-T X.800 (03/1991), 1991, 3.3.55**
Intergovernmental Organization (Glossary or specific definition listed in document)

[10] Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (See: logic bomb, Trojan horse, spyware, virus, worm. Compare: secondary definitions "corruption", "incapacitation", "masquerade", and "misuse".)

1a. (I) A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. (See: dangling threat, INFOCON level, threat action, threat agent, threat consequence. Compare: attack, vulnerability.)
1b. (N) Any circumstance or event with the potential to adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service. (See: sensitive information.)
Usage: (a) Frequently misused with the meaning of either "threat action" or "vulnerability". (b) In some contexts, "threat" is used more narrowly to refer only to intelligent threats; for example, see definition 2 below. (c) In some contexts, "threat" is used more broadly to cover both definition 1 and other concepts, such as in definition 3 below.
Tutorial: A threat is a possible danger that might exploit a vulnerability. Thus, a threat may be intentional or not:
- "Intentional threat": A possibility of an attack by an intelligent entity (e.g., an individual cracker or a criminal organization).
- "Accidental threat": A possibility of human error or omission, unintended equipment malfunction, or natural disaster (e.g., fire, flood, earthquake, windstorm, and other causes listed in).
The Common Criteria characterizes a threat in terms of (a) a threat agent, (b) a presumed method of attack, (c) any vulnerabilities that are the foundation for the attack, and (d) the system resource that is attacked. That characterization agrees with the definitions in this Glossary (see: diagram under "attack").
2. (O) The technical and operational ability of a hostile entity to detect, exploit, or subvert a friendly system and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.
Tutorial: To be likely to launch an attack, an adversary must have (a) a motive to attack, (b) a method or technical ability to make the attack, and (c) an opportunity to appropriately access the targeted system.
3. (D) "An indication of an impending undesirable event."
Deprecated Definition: IDOCs SHOULD NOT use this term with definition 3 because the definition is ambiguous; the definition was intended to include the following three meanings:
- "Potential threat": A possible security violation; i.e., the same as definition 1.
- "Active threat": An expression of intent to violate security. (Context usually distinguishes this meaning from the previous one.)
- "Accomplished threat" or "actualized threat": That is, a threat action. Deprecated Usage: IDOCs SHOULD NOT use the term "threat" with this meaning; instead, use "threat action".
**- Internet Engineering Task Force, Internet Security Glossary Version 2, 2007**
Other Source (Glossary or specific definition listed in document)

Any action intended to breach the security of information stored in a system by (a) gaining unauthorized access to that information usually without alerting the authorized user; (b) denial of service to the authorized user; (c) spoofing, which aims to confuse by introducing false information, usually as to the identity of the user. Some threats are with premeditated malicious intent but others are opportunistic, e.g. browsing, or occur during a crash.
**- Oxford University, A Dictionary of Computing, 2004, p. 535**
Other Source (Dictionary)

# TABLES

## I. Number of Citations by Term and Source – General

| Source | Computer | Computer System | Information | Information and Communication Technologies | Information System | Information Technology | Information Technology and Communication | the Internet |
|---|---|---|---|---|---|---|---|---|
| **Total** | 2 | 2 | 12 | 6 | 14 | 8 | 1 | 6 |
| African Union | | | 1 | | | | | |
| Armenia | | | | | | | | |
| Australia | | | | 1 | | | | |
| Austria | | | | 1 | | | | |
| Azerbaijan | | | | | 1 | 1 | | |
| Belarus | | | | | 1 | 1 | | |
| Belgium | | | | | | | | |
| Bolivia | | | 1 | | | | | |
| Brunei | | | | | | 1 | | |
| Canada | | | | | | | | |
| China | | | | | | | | |
| Colombia | | | | 1 | | | | |
| Commonwealth of Independent States | | | | | | | | |
| Council of Europe | | 1 | | | 1 | | | |
| Cuba | | | | | | | | |
| Czech Republic | | | | | | | | |
| Denmark | | | | | | | | |
| EastWest Institute | | | | | | | | |
| Economic Community of West African States | | | | | | | 1 | |
| Ecuador | | | | | | | | |
| Estonia | | | | | | | | |
| European Union | | | | | | | | |
| Finland | | | | | 1 | | | |
| France | | | | | 1 | | | |
| Georgia | | | | | | | | |
| Germany | | | | | | 1 | | 1 |
| Ghana | | | | | | | | |
| Hungary | | | 1 | | | | | |
| India | 1 | | 1 | | | | | |
| Institute of Electrical and Electronic Engineers | | | 1 | | | | | |
| International Organization for Standardization | | | | | 1 | | | 1 |
| International Telecommunication Union | | | 2 | 1 | 2 | | | 1 |
| Internet Engineering Task Force | | | 1 | | 1 | | | 1 |
| Internet Society | | | | | | | | |

| Source | Computer | Computer System | Information | Information and Communication Technologies | Information System | Information Technology | Information Technology and Communication | the Internet |
|---|---|---|---|---|---|---|---|---|
| Israel | | | | | | | | |
| Italy | | | | | | | | |
| Japan | | | | | | | | |
| Jordan | | | | | | | | |
| Kazakhstan | | | | | | | | |
| Kenya | | | | 1 | | | | |
| Latvia | | | | | | | | |
| League of Arab States | | | | | | 1 | | |
| Lebanon | | | | | | | | |
| Lithuania | | | | | | | | |
| Mali | | | | | | | | |
| Mongolia | | | | | | | | |
| Montenegro | | | | | | | | |
| Netherlands | | | | | | | | |
| New Zealand | | | | | | | | |
| North Atlantic Treaty Organization | | 1 | | | | | | |
| Norway | | | | | 1 | | | |
| Oman | | | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | | | |
| Oxford Dictionary of Computing (2004) | 1 | | 1 | | | | | 1 |
| Oxford Dictionary of Computing (2008) | | | 1 | | 1 | 1 | | |
| Oxford English Dictionary | | | | | | | | |
| Panama | | | | | | | | |
| Philippines | | | | | | | | |
| Poland | | | | | | | | |
| Qatar | | | | | | | | |
| Romania | | | | | | | | |
| Russia | | | | | | | | |
| Saudi Arabia | | | | | | | | |
| Serbia | | | | | | | | |
| Shanghai Cooperation Organization | | | | | | | | |
| South Africa | | | | | | | | |
| South Korea | | | | | | | | |
| Spain | | | | | | | | |
| Sweden | | | | | | | | |
| Switzerland | | | | | | | | |

| Source | Computer | Computer System | Information | Information and Communication Technologies | Information System | Information Technology | Information Technology and Communication | the Internet |
|---|---|---|---|---|---|---|---|---|
| Turkey | | | | | 1 | | | |
| Uganda | | | | | | | | |
| Ukraine | | | | | | | | |
| United Kingdom | | | | | | | | |
| United States of America | | | 2 | 1 | 2 | 2 | | 1 |
| Venezuela | | | | | | | | |

## II. Number of Citations by Term and Source – Space

| Source | Cyber Domain | Cyber Environment | Cyber space | Information Area | Information Environment | Information Space | Information Sphere |
|---|---|---|---|---|---|---|---|
| **Total** | 1 | 1 | 45 | 1 | 2 | 4 | 2 |
| African Union | | | | | | | |
| Armenia | | | | | | | |
| Australia | | | | | | | |
| Austria | | | 1 | | | | |
| Azerbaijan | | | | | | | |
| Belarus | | | | | | | |
| Belgium | | | 1 | | | | |
| Bolivia | | | | | | | |
| Brunei | | | | | | | |
| Canada | | | 1 | | | | |
| China | | | | | | | |
| Colombia | | | 1 | | | | |
| Commonwealth of Independent States | | | | | | | |
| Council of Europe | | | | | | | |
| Cuba | | | | | | | |
| Czech Republic | | | 1 | | | | |
| Denmark | | | | | | | |
| EastWest Institute | | | 1 | | | 1 | |
| Economic Community of West African States | | | | | | | |
| Ecuador | | | | | | | |
| Estonia | | | | | | | |
| European Union | | | | | | | |
| Finland | 1 | | | | | | |
| France | | | 1 | | | | |
| Georgia | | | | | | | |
| Germany | | | 4 | | | | |
| Ghana | | | | | | | |
| Hungary | | | 1 | | | | |
| India | | | 1 | | | | |
| Institute of Electrical and Electronic Engineers | | | | | | | |
| International Organization for Standardization | | | 1 | | | 1 | |
| International Telecommunication Union | | 1 | | | | | |
| Internet Engineering Task Force | | | | | | | |
| Internet Society | | | | | | | |
| Israel | | | 1 | | | | |
| Italy | | | 1 | | | | |
| Japan | | | 2 | | | | |
| Jordan | | | | | | | |
| Kazakhstan | | | | | | | |
| Kenya | | | 1 | | | | |
| Latvia | | | | | | | |

| Source | Cyber Domain | Cyber Environment | Cyber space | Information Area | Information Environment | Information Space | Information Sphere |
|---|---|---|---|---|---|---|---|
| League of Arab States | | | | | | | |
| Lebanon | | | 1 | | | | |
| Lithuania | | | 1 | | 1 | | |
| Mali | | | | | | | |
| Mongolia | | | | | | | |
| Montenegro | | | 1 | | | | |
| Netherlands | | | 1 | | | | |
| New Zealand | | | 1 | | | | |
| North Atlantic Treaty Organization | | | 1 | | | | |
| Norway | | | | | | | |
| Oman | | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | | |
| Oxford Dictionary of Computing (2004) | | | 1 | | | | |
| Oxford Dictionary of Computing (2008) | | | 1 | | | | |
| Oxford English Dictionary | | | 1 | | | | |
| Panama | | | | | | | |
| Philippines | | | | | | | |
| Poland | | | 1 | | | | |
| Qatar | | | | | | | |
| Romania | | | 1 | | | | |
| Russia | | | 1 | 1 | | 2 | 1 |
| Saudi Arabia | | | 1 | | | | |
| Serbia | | | | | | | |
| Shanghai Cooperation Organization | | | | | | | |
| South Africa | | | 1 | | | | 1 |
| South Korea | | | | | | | |
| Spain | | | 1 | | | | |
| Sweden | | | | | | | |
| Switzerland | | | 1 | | | | |
| Turkey | | | 1 | | | | |
| Uganda | | | | | | | |
| Ukraine | | | | | | | |
| United Kingdom | | | 2 | | | | |
| United States of America | | | 7 | | 1 | | |
| Venezuela | | | | | | | |

## III. Number of Citations by Term and Source – Security

| Source | Computer Security | Cybersecurity | Information Security | IT Security | Information System Security | International Information Security | Internet Security | Security | Security of Information |
|---|---|---|---|---|---|---|---|---|---|
| **Total** | 5 | 49 | 33 | 3 | 1 | 2 | 1 | 8 | 2 |
| African Union | | | | | | | | | |
| Armenia | | | 1 | | | | | | |
| Australia | | 1 | 1 | | | | | | |
| Austria | | 2 | 1 | | | | | | |
| Azerbaijan | | | | | | | | | |
| Belarus | | | 1 | | | | | | |
| Belgium | | 1 | | | | | | | |
| Bolivia | | | | | | | | | |
| Brunei | | | | | | | | | |
| Canada | | | | | | | | | |
| China | | | 2 | | | | | | |
| Colombia | | 1 | | | | | | | |
| Commonwealth of Independent States | | | | | | | | | |
| Council of Europe | | | | | | | | | |
| Cuba | | | | | | | | | 1 |
| Czech Republic | | 1 | | | | | | | 1 |
| Denmark | | | | | | | | | |
| EastWest Institute | | 1 | 1 | | | | | | |
| Economic Community of West African States | | | | | | | | | |
| Ecuador | | | | | | | | | |
| Estonia | | 1 | 1 | | | | | | |
| European Union | | 1 | | | | | | | |
| Finland | | 1 | 1 | | | | | | |
| France | | 1 | | | 1 | | | | |
| Georgia | | 1 | | | | | | | |
| Germany | | 3 | | 3 | | | | | |
| Ghana | | 1 | | | | | | | |
| Hungary | | 2 | | | | | | | |
| India | | 2 | | | | | | | |
| Institute of Electrical and Electronic Engineers | 2 | 1 | | | | | | | |
| International Organization for Standardization | | 2 | 1 | | | | | 2 | |
| International Telecommunication Union | | 2 | | | | | | 3 | |
| Internet Engineering Task Force | 1 | | 1 | | | | | 1 | |
| Internet Society | | 1 | | | | | | | |
| Israel | | 1 | | | | | | | |
| Italy | | 1 | | | | | | | |
| Japan | | 1 | 2 | | | | | | |

| Source | Computer Security | Cybersecurity | Information Security | IT Security | Information System Security | International Information Security | Internet Security | Security | Security of Information |
|---|---|---|---|---|---|---|---|---|---|
| Jordan | | | 2 | | | | | | |
| Kazakhstan | | | | | | | | | |
| Kenya | | 1 | | | | | | | |
| Latvia | | | | | | | | | |
| League of Arab States | | | | | | | | | |
| Lebanon | | | | | | | | | |
| Lithuania | | 1 | | | | | | | |
| Mali | | | | | | 1 | | | |
| Mongolia | | | 1 | | | | | | |
| Montenegro | | 1 | 1 | | | | 1 | | |
| Netherlands | | 1 | | | | | | | |
| New Zealand | | 1 | | | | | | | |
| North Atlantic Treaty Organization | | | | | | | | | |
| Norway | | 1 | 1 | | | | | | |
| Oman | | | 1 | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | | | | |
| Oxford Dictionary of Computing (2004) | | | | | | | | 1 | |
| Oxford Dictionary of Computing (2008) | | | | | | | | | |
| Oxford English Dictionary | | 1 | | | | | | | |
| Panama | | | | | | | | | |
| Philippines | | | | | | | | | |
| Poland | | | | | | | | | |
| Qatar | | | 1 | | | | | | |
| Romania | | 1 | | | | | | | |
| Russia | | 1 | 4 | | | 1 | | | |
| Saudi Arabia | | 1 | | | | | | | |
| Serbia | | | 1 | | | | | | |
| Shanghai Cooperation Organization | | | | | | | | | |
| South Africa | | 1 | | | | | | | |
| South Korea | | | | | | | | | |
| Spain | | | | | | | | | |
| Sweden | | 1 | | | | | | | |
| Switzerland | | | | | | | | | |
| Turkey | | 1 | | | | | | | |
| Uganda | | | 1 | | | | | | |
| Ukraine | | | 2 | | | | | | |
| United Kingdom | | 2 | 2 | | | | | | |
| United States of America | 2 | 5 | 2 | | | | | 1 | |
| Venezuela | | | 1 | | | | | | |

## IV. Number of Citations by Term and Source – Incident

| Source | Cyber Incident | Information and Communication Networks (ICN) Security Incident | Information Incident | Information Security Event | Information Security Incident | Information Technologies Security Incident | Security Incident |
|---|---|---|---|---|---|---|---|
| **Total** | 6 | 1 | 1 | 2 | 3 | 1 | 3 |
| African Union | | | | | | | |
| Armenia | | | | | | | |
| Australia | | | | | | | |
| Austria | | | | | | | |
| Azerbaijan | | | | | | | |
| Belarus | | | | | | | |
| Belgium | | | | | | | |
| Bolivia | | | | | | | |
| Brunei | | | | | | | |
| Canada | | | | | | | |
| China | | | | | | | |
| Colombia | | | 1 | | | | |
| Commonwealth of Independent States | | | | | | | |
| Council of Europe | | | | | | | |
| Cuba | | | | | | | |
| Czech Republic | 1 | | | | | | |
| Denmark | | | | | | | |
| EastWest Institute | | | | | | | |
| Economic Community of West African States | | | | | | | |
| Ecuador | | | | | | | |
| Estonia | | | | | | | |
| European Union | | | | | | | |
| Finland | | | | | | | |
| France | | | | | | | |
| Georgia | | | | | | | |
| Germany | | | | | | | |
| Ghana | | | | | | | |
| Hungary | | | | | | | |
| India | 1 | | | | | | |
| Institute of Electrical and Electronic Engineers | | | | | | | |
| International Organization for Standardization | | 1 | | 2 | 3 | | 2 |
| International Telecommunication Union | | | | | | | |
| Internet Engineering Task Force | | | | | | | 1 |
| Internet Society | | | | | | | |
| Israel | | | | | | | |
| Italy | | | | | | | |
| Japan | | | | | | | |
| Jordan | | | | | | | |
| Kazakhstan | | | | | | | |
| Kenya | | | | | | | |
| Latvia | | | | | | 1 | |

| Source | Cyber Incident | Information and Communication Networks (ICN) Security Incident | Information Incident | Information Security Event | Information Security Incident | Information Technologies Security Incident | Security Incident |
|---|---|---|---|---|---|---|---|
| League of Arab States | | | | | | | |
| Lebanon | | | | | | | |
| Lithuania | 1 | | | | | | |
| Mali | | | | | | | |
| Mongolia | | | | | | | |
| Montenegro | | | | | | | |
| Netherlands | | | | | | | |
| New Zealand | | | | | | | |
| North Atlantic Treaty Organization | | | | | | | |
| Norway | | | | | | | |
| Oman | | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | | |
| Oxford Dictionary of Computing (2004) | | | | | | | |
| Oxford Dictionary of Computing (2008) | | | | | | | |
| Oxford English Dictionary | | | | | | | |
| Panama | | | | | | | |
| Philippines | | | | | | | |
| Poland | | | | | | | |
| Qatar | | | | | | | |
| Romania | 1 | | | | | | |
| Russia | | | | | | | |
| Saudi Arabia | | | | | | | |
| Serbia | | | | | | | |
| Shanghai Cooperation Organization | | | | | | | |
| South Africa | | | | | | | |
| South Korea | | | | | | | |
| Spain | | | | | | | |
| Sweden | | | | | | | |
| Switzerland | | | | | | | |
| Turkey | | | | | | | |
| Uganda | | | | | | | |
| Ukraine | | | | | | | |
| United Kingdom | | | | | | | |
| United States of America | 2 | | | | | | |
| Venezuela | | | | | | | |

## V. Number of Citations by Term and Source – Critical Infrastructure

| Source | Critical | Critical ICT Infrastructure | Critical Information Infrastructure | Critical Infrastructure | Critical Infrastructure and Key Resources | Critical National Infrastructure | Cyber Infrastructure | Electronic Information Infrastructure | Global Information Infrastructure | ICT Infrastructure | Information Infrastructure | National Critical Infrastructure and Key Assets | Vital Structures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Total** | 2 | 1 | 4 | 18 | 1 | 1 | 3 | 1 | 1 | 1 | 2 | 1 | 2 |
| African Union | | | | | | | | | | | | | |
| Armenia | | | | | | | | | | | | | |
| Australia | | | | 1 | | | | | | | | | |
| Austria | | | | 1 | | | | | | | | | |
| Azerbaijan | | | | | | | | | | | | | |
| Belarus | | | | | | | | | | | | | |
| Belgium | | | | | | | | | | | | | |
| Bolivia | | | | | | | | | | | | | |
| Brunei | | | | | | | | | | | | | |
| Canada | | | | 1 | | | | | | | | | |
| China | | | | | | | | | | | | | |
| Colombia | | | | 1 | | | | | | | | | |
| Commonwealth of Independent States | | | | | | | | | | | | | |
| Council of Europe | | | | | | | | | | | | | |
| Cuba | | | | | | | | | | | | | |
| Czech Republic | | | 1 | | | | | | | | | | |
| Denmark | | | | | | | | | | | | | |
| EastWest Institute | | | | | | | 1 | | | | | | |
| Economic Community of West African States | | | | | | | | | | | | | |
| Ecuador | | | | | | | | | | | | | |
| Estonia | | | | | | | | | | | | | |
| European Union | | | | | | | | | | | | | |
| Finland | | | | | | | | | | | | | |
| France | | | | | | | | | | | | | |

| Source | Critical | Critical ICT Infrastructure | Critical Information Infrastructure | Critical Infrastructure | Critical Infrastructure and Key Resources | Critical National Infrastructure | Cyber Infrastructure | Electronic Information Infrastructure | Global Information Infrastructure | ICT Infrastructure | Information Infrastructure | National Critical Infrastructure and Key Assets | Vital Structures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Georgia | | | | | | | | | | | | | |
| Germany | | | | 1 | | | | | | | 1 | | |
| Ghana | | | | | | | | | | | | | |
| Hungary | | | | | | | | 1 | | | | | |
| India | | | | | | | | | | | | | |
| Institute of Electrical and Electronic Engineers | | | | | | | | | | | | | |
| International Organization for Standardization | 1 | | | 1 | | | | | | | | | |
| International Telecom. Union | | | | | | | | | 1 | | | | |
| Internet Engineering Task Force | 1 | | 1 | | | | | | | | | | |
| Internet Society | | | | | | | | | | | | | |
| Israel | | | | | | | | | | | | | |
| Italy | | | | 1 | | | | | | | | | |
| Japan | | | | 1 | | | | | | | | | |
| Jordan | | | | | | | | | | | | | |
| Kazakhstan | | | | | | | | | | | | | |
| Kenya | | | | | | | | | | | | | |
| Latvia | | | | | | | | | | | | | |
| League of Arab States | | | | | | | | | | | | | |
| Lebanon | | | | | | | | | | | | | |
| Lithuania | | | 1 | | | | | | | | | | |
| Mali | | | | | | | | | | | | | |
| Mongolia | | | | | | | | | | | | | |
| Montenegro | | | | | | | | | | | | | |
| Netherlands | | | | | | | | | | | | | |
| New Zealand | | | | | | 1 | | | | | | | |
| NATO | | | | 1 | | | | | | | | | |

| Source | Critical | Critical ICT Infrastructure | Critical Information Infrastructure | Critical Infrastructure | Critical Infrastructure and Key Resources | Critical National Infrastructure | Cyber Infrastructure | Electronic Information Infrastructure | Global Information Infrastructure | ICT Infrastructure | Information Infrastructure | National Critical Infrastructure and Key Assets | Vital Structures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Norway | | 1 | | 1 | | | | | | 1 | | | |
| Oman | | | | | | | | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | | | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | | | | | | | | |
| Oxford Dictionary of Computing (2004) | | | | | | | | | | | | | |
| Oxford Dictionary of Computing (2008) | | | | | | | | | | | | | |
| Oxford English Dictionary | | | | | | | | | | | | | |
| Panama | | | | | | | | | | | | | |
| Philippines | | | | | | | | | | | | | |
| Poland | | | | | | | | | | | | | |
| Qatar | | | | | | | | | | | | | |
| Romania | | | | | | | | | | | | | |
| Russia | | | | | | | | | | | 1 | | 2 |
| Saudi Arabia | | | | 1 | | | | | | | | | |
| Serbia | | | | | | | | | | | | | |
| Shanghai Cooperation Organization | | | | | | | | | | | | | |
| South Africa | | | | | | | | | | | | | |
| South Korea | | | | | | | | | | | | | |
| Spain | | | | | | | | | | | | | |
| Sweden | | | | | | | | | | | | | |
| Switzerland | | | | 1 | | | | | | | | | |
| Turkey | | | | 1 | | | | | | | | | |
| Uganda | | | | | | | | | | | | | |

| Source | Critical | Critical ICT Infrastructure | Critical Information Infrastructure | Critical Infrastructure | Critical Infrastructure and Key Resources | Critical National Infrastructure | Cyber Infrastructure | Electronic Information Infrastructure | Global Information Infrastructure | ICT Infrastructure | Information Infrastructure | National Critical Infrastructure and Key Assets | Vital Structures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ukraine | | | | | | | | | | | | | |
| United Kingdom | | | 1 | | | | | | | | | | |
| United States of America | | | | 5 | 1 | | 2 | | | | 1 | | |
| Venezuela | | | | | | | | | | | | | |

## VI. Number of Citations by Term and Source – Weapon

| Source | Cyber Weapon | Information Weapon | Use of the Internet as a Weapon |
|---|---|---|---|
| **Total** | 2 | 6 | 1 |
| African Union | | | |
| Armenia | | | |
| Australia | | | |
| Austria | | | |
| Azerbaijan | | | |
| Belarus | | | |
| Belgium | | | |
| Bolivia | | | |
| Brunei | | | |
| Canada | | | |
| China | | | |
| Colombia | | | |
| Commonwealth of Independent States | | | |
| Council of Europe | | | |
| Cuba | | 2 | |
| Czech Republic | | | |
| Denmark | | | |
| EastWest Institute | 1 | | |
| Economic Community of West African States | | | |
| Ecuador | | | |
| Estonia | | | |
| European Union | | | |
| Finland | | | |
| France | | | |
| Georgia | | | |
| Germany | | | |
| Ghana | | | |
| Hungary | | | |
| India | | | |
| Institute of Electrical and Electronic Engineers | | | |
| International Organization for Standardization | | | |
| International Telecommunication Union | | | |
| Internet Engineering Task Force | | | |
| Internet Society | | | |
| Israel | | | |
| Italy | | | |
| Japan | | | |
| Jordan | | | |
| Kazakhstan | | | |
| Kenya | | | |
| Latvia | | | |

| Source | Cyber Weapon | Information Weapon | Use of the Internet as a Weapon |
|---|---|---|---|
| League of Arab States | | | |
| Lebanon | | | |
| Lithuania | | | |
| Mali | | | |
| Mongolia | | | |
| Montenegro | | | |
| Netherlands | | | |
| New Zealand | | | |
| North Atlantic Treaty Organization | | | |
| Norway | | | |
| Oman | | | |
| Organization for Economic Cooperation and Development | 1 | | |
| Organization for Security and Cooperation in Europe | | | |
| Oxford Dictionary of Computing (2004) | | | |
| Oxford Dictionary of Computing (2008) | | | |
| Oxford English Dictionary | | | |
| Panama | | | |
| Philippines | | 1 | |
| Poland | | | |
| Qatar | | | |
| Romania | | | |
| Russia | | 3 | |
| Saudi Arabia | | | |
| Serbia | | | |
| Shanghai Cooperation Organization | | | |
| South Africa | | | |
| South Korea | | | |
| Spain | | | 1 |
| Sweden | | | |
| Switzerland | | | |
| Turkey | | | |
| Uganda | | | |
| Ukraine | | | |
| United Kingdom | | | |
| United States of America | | | |
| Venezuela | | | |

## VII. Number of Citations by Term and Source – Crime

| Source | Cyber Crimes or Information Crimes | Cybercrime | Information Crime | Internet Crime |
|---|---|---|---|---|
| **Total** | 1 | 20 | 1 | 1 |
| African Union | | | | |
| Armenia | | | | |
| Australia | | 1 | | |
| Austria | | 1 | | |
| Azerbaijan | | | | |
| Belarus | | | | |
| Belgium | | 1 | | |
| Bolivia | | | | |
| Brunei | | | | |
| Canada | | | | |
| China | | | | |
| Colombia | | 2 | | |
| Commonwealth of Independent States | | | | |
| Council of Europe | | | | |
| Cuba | | | | |
| Czech Republic | | | | |
| Denmark | | | | |
| EastWest Institute | | 1 | | |
| Economic Community of West African States | | | | |
| Ecuador | | 1 | | |
| Estonia | | 1 | | |
| European Union | | 1 | | |
| Finland | | | | |
| France | | 1 | | |
| Georgia | | | | |
| Germany | | 2 | | |
| Ghana | | | | |
| Hungary | | | | |
| India | | | | |
| Institute of Electrical and Electronic Engineers | | | | |
| International Organization for Standardization | | 1 | | 1 |
| International Telecommunication Union | | | | |
| Internet Engineering Task Force | | | | |
| Internet Society | | | | |
| Israel | | | | |
| Italy | | | | |
| Japan | | | | |
| Jordan | | | | |
| Kazakhstan | | 1 | | |
| Kenya | | | | |
| Latvia | | | | |

| Source | Cyber Crimes or Information Crimes | Cybercrime | Information Crime | Internet Crime |
|---|---|---|---|---|
| League of Arab States | | | | |
| Lebanon | | | | |
| Lithuania | | | | |
| Mali | | | | |
| Mongolia | | | | |
| Montenegro | | | | |
| Netherlands | | | | |
| New Zealand | | 1 | | |
| North Atlantic Treaty Organization | | | | |
| Norway | | | | |
| Oman | | | | |
| Organization for Economic Cooperation and Development | | | | |
| Organization for Security and Cooperation in Europe | | | | |
| Oxford Dictionary of Computing (2004) | | | | |
| Oxford Dictionary of Computing (2008) | | 1 | | |
| Oxford English Dictionary | | | | |
| Panama | | | | |
| Philippines | 1 | | | |
| Poland | | 1 | | |
| Qatar | | | | |
| Romania | | | 1 | |
| Russia | | | | |
| Saudi Arabia | | | | |
| Serbia | | | | |
| Shanghai Cooperation Organization | | | | |
| South Africa | | 2 | | |
| South Korea | | | | |
| Spain | | | | |
| Sweden | | | | |
| Switzerland | | | | |
| Turkey | | | | |
| Uganda | | | | |
| Ukraine | | | | |
| United Kingdom | | 1 | | |
| United States of America | | | | |
| Venezuela | | | | |

## VIII. Number of Citations by Term and Source – Espionage & Sabotage

| Source | Cyber Espionage | Cyber Sabotage |
|---|---|---|
| **Total** | 9 | 2 |
| African Union | | |
| Armenia | | |
| Australia | | |
| Austria | 1 | 1 |
| Azerbaijan | | |
| Belarus | | |
| Belgium | | |
| Bolivia | | |
| Brunei | | |
| Canada | | |
| China | | |
| Colombia | | |
| Commonwealth of Independent States | | |
| Council of Europe | | |
| Cuba | | |
| Czech Republic | | |
| Denmark | | |
| EastWest Institute | 1 | |
| Economic Community of West African States | | |
| Ecuador | | |
| Estonia | | |
| European Union | | |
| Finland | | |
| France | | |
| Georgia | | |
| Germany | 1 | 1 |
| Ghana | | |
| Hungary | | |
| India | | |
| Institute of Electrical and Electronic Engineers | | |
| International Organization for Standardization | | |
| International Telecommunication Union | | |
| Internet Engineering Task Force | | |
| Internet Society | | |
| Israel | | |
| Italy | | |
| Japan | | |
| Jordan | | |
| Kazakhstan | | |
| Kenya | | |
| Latvia | | |
| League of Arab States | | |
| Lebanon | | |

| Source | Cyber Espionage | Cyber Sabotage |
|---|---|---|
| Lithuania | | |
| Mali | | |
| Mongolia | | |
| Montenegro | 1 | |
| Netherlands | | |
| New Zealand | | |
| North Atlantic Treaty Organization | 1 | |
| Norway | | |
| Oman | | |
| Organization for Economic Cooperation and Development | | |
| Organization for Security and Cooperation in Europe | | |
| Oxford Dictionary of Computing (2004) | | |
| Oxford Dictionary of Computing (2008) | | |
| Oxford English Dictionary | 1 | |
| Panama | | |
| Philippines | | |
| Poland | | |
| Qatar | | |
| Romania | 1 | |
| Russia | | |
| Saudi Arabia | | |
| Serbia | | |
| Shanghai Cooperation Organization | | |
| South Africa | 1 | |
| South Korea | | |
| Spain | | |
| Sweden | | |
| Switzerland | | |
| Turkey | | |
| Uganda | | |
| Ukraine | | |
| United Kingdom | 1 | |
| United States of America | | |
| Venezuela | | |

## IX. Number of Citations by Term and Source – Terrorism

| Source | Cyber Terrorism | Information Terrorism | International Information Terrorism | Use of the Internet for Terrorist Purposes |
|---|---|---|---|---|
| **Total** | 11 | 2 | 1 | 1 |
| African Union | | | | |
| Armenia | | | | |
| Australia | | | | |
| Austria | 1 | | | |
| Azerbaijan | | | | |
| Belarus | | | | |
| Belgium | | | | |
| Bolivia | | | | |
| Brunei | | | | |
| Canada | 1 | | | |
| China | | | | |
| Colombia | 1 | | | |
| Commonwealth of Independent States | | | | |
| Council of Europe | | | | |
| Cuba | | | | |
| Czech Republic | | | | |
| Denmark | | | | |
| EastWest Institute | 1 | | | |
| Economic Community of West African States | | | | |
| Ecuador | | | | |
| Estonia | | | | |
| European Union | | | | |
| Finland | | | | |
| France | | | | |
| Georgia | | | | |
| Germany | | | | |
| Ghana | | | | |
| Hungary | | | | |
| India | | | | |
| Institute of Electrical and Electronic Engineers | | | | |
| International Organization for Standardization | | | | |
| International Telecommunication Union | | | | |
| Internet Engineering Task Force | | | | |
| Internet Society | | | | |
| Israel | | | | |
| Italy | 1 | | | |
| Japan | | | | |
| Jordan | | | | |
| Kazakhstan | | | | |
| Kenya | | | | |
| Latvia | | | | |
| League of Arab States | | | | |

| Source | Cyber Terrorism | Information Terrorism | International Information Terrorism | Use of the Internet for Terrorist Purposes |
|---|---|---|---|---|
| Lebanon | | | | |
| Lithuania | | | | |
| Mali | | | | |
| Mongolia | | | | |
| Montenegro | 1 | | | |
| Netherlands | | | | |
| New Zealand | | | | |
| North Atlantic Treaty Organization | | | | |
| Norway | | | | |
| Oman | | | | |
| Organization for Economic Cooperation and Development | | | | |
| Organization for Security and Cooperation in Europe | 1 | | | |
| Oxford Dictionary of Computing (2004) | | | | |
| Oxford Dictionary of Computing (2008) | | | | |
| Oxford English Dictionary | 1 | | | |
| Panama | | | | 1 |
| Philippines | | 1 | | |
| Poland | 1 | | | |
| Qatar | | | | |
| Romania | 1 | | | |
| Russia | | | 1 | |
| Saudi Arabia | | | | |
| Serbia | | | | |
| Shanghai Cooperation Organization | | 1 | | |
| South Africa | | | | |
| South Korea | 1 | | | |
| Spain | | | | |
| Sweden | | | | |
| Switzerland | | | | |
| Turkey | | | | |
| Uganda | | | | |
| Ukraine | | | | |
| United Kingdom | | | | |
| United States of America | | | | |
| Venezuela | | | | |

## X. Number of Citations by Term and Source – War & Warfare

| Source | Cyber War | Cyber Warfare | Information War | Information Warfare |
|---|---|---|---|---|
| **Total** | 7 | 3 | 4 | 2 |
| African Union | | | | |
| Armenia | | | | |
| Australia | | | | |
| Austria | 1 | | | |
| Azerbaijan | | | | |
| Belarus | | | | |
| Belgium | 1 | | | |
| Bolivia | | | | |
| Brunei | | | | |
| Canada | | | | |
| China | | | | |
| Colombia | | | | |
| Commonwealth of Independent States | | | | |
| Council of Europe | | | | |
| Cuba | | | | |
| Czech Republic | | | | |
| Denmark | | | | |
| EastWest Institute | 1 | 1 | 1 | |
| Economic Community of West African States | | | | |
| Ecuador | | | | |
| Estonia | | | | |
| European Union | | | | |
| Finland | | | | |
| France | | | | |
| Georgia | | | | |
| Germany | | | | |
| Ghana | | | | |
| Hungary | | | | |
| India | | | | |
| Institute of Electrical and Electronic Engineers | | | | |
| International Organization for Standardization | | | | |
| International Telecommunication Union | | | | |
| Internet Engineering Task Force | | | | |
| Internet Society | | | | |
| Israel | | | | |
| Italy | | 1 | | |
| Japan | | | | |
| Jordan | | | | |
| Kazakhstan | | | | |
| Kenya | | | | |
| Latvia | | | | |
| League of Arab States | | | | |

| Source | Cyber War | Cyber Warfare | Information War | Information Warfare |
|---|---|---|---|---|
| Lebanon | | | | |
| Lithuania | | | | |
| Mali | | | | |
| Mongolia | | | | |
| Montenegro | 1 | | | |
| Netherlands | | | | |
| New Zealand | | | | |
| North Atlantic Treaty Organization | | | | |
| Norway | | | | |
| Oman | | | | |
| Organization for Economic Cooperation and Development | 2 | | | |
| Organization for Security and Cooperation in Europe | | | | |
| Oxford Dictionary of Computing (2004) | | | | |
| Oxford Dictionary of Computing (2008) | | | | |
| Oxford English Dictionary | 1 | | | |
| Panama | | | | |
| Philippines | | | | 1 |
| Poland | | | | |
| Qatar | | | | |
| Romania | | | | |
| Russia | | | 3 | |
| Saudi Arabia | | | | |
| Serbia | | | | |
| Shanghai Cooperation Organization | | | | |
| South Africa | | 1 | | 1 |
| South Korea | | | | |
| Spain | | | | |
| Sweden | | | | |
| Switzerland | | | | |
| Turkey | | | | |
| Uganda | | | | |
| Ukraine | | | | |
| United Kingdom | | | | |
| United States of America | | | | |
| Venezuela | | | | |

## XI. Number of Citations by Term and Source – Others – Part 1/3

| Source | Attack | Attacker | Computer Network Attack | Computer Network Defense | Computer Network Exploitation | Computer Network Operations |
|---|---|---|---|---|---|---|
| **Total** | 7 | 3 | 4 | 4 | 3 | 5 |
| African Union | | | | | | |
| Armenia | | | | | | |
| Australia | | | | | | |
| Austria | | | | | | |
| Azerbaijan | | | | | | |
| Belarus | | | | | | |
| Belgium | | | | | | |
| Bolivia | | | | | | |
| Brunei | | | | | | |
| Canada | | | | | | |
| China | | | | | | |
| Colombia | | | | | | |
| Commonwealth of Independent States | | | | | | |
| Council of Europe | | | | | | |
| Cuba | | | | | | |
| Czech Republic | | | | | | |
| Denmark | | | | | | 1 |
| EastWest Institute | | | | | | |
| Economic Community of West African States | | | | | | |
| Ecuador | | | | | | |
| Estonia | | | | | | |
| European Union | | | | | | |
| Finland | | | | | | |
| France | | | | | | |
| Georgia | | | | | | |
| Germany | 1 | | | | | |
| Ghana | | | | | | |
| Hungary | | | | | | |
| India | | | | | | |
| Institute of Electrical and Electronic Engineers | | | | | | |
| International Organization for Standardization | 2 | 3 | | | | |
| International Telecommunication Union | 2 | | | | | |
| Internet Engineering Task Force | 1 | | | | | |
| Internet Society | | | | | | |
| Israel | | | | | | |
| Italy | | | 1 | 1 | 1 | 1 |
| Japan | | | | | | |
| Jordan | | | | | | |
| Kazakhstan | | | | | | |
| Kenya | | | | | | |
| Latvia | | | | | | |

| Source | Attack | Attacker | Computer Network Attack | Computer Network Defense | Computer Network Exploitation | Computer Network Operations |
|---|---|---|---|---|---|---|
| League of Arab States | | | | | | |
| Lebanon | | | | | | |
| Lithuania | | | | | | |
| Mali | | | | | | |
| Mongolia | | | | | | |
| Montenegro | | | | | | |
| Netherlands | | | | | | |
| New Zealand | | | | | | |
| North Atlantic Treaty Organization | | | 1 | | | |
| Norway | | | | | | |
| Oman | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | |
| Oxford Dictionary of Computing (2004) | | | | | | |
| Oxford Dictionary of Computing (2008) | | | | | | |
| Oxford English Dictionary | | | | | | |
| Panama | | | | | | |
| Philippines | | | | | | |
| Poland | | | | | | |
| Qatar | | | | | | |
| Romania | | | | | | 1 |
| Russia | | | | | | |
| Saudi Arabia | | | | | | |
| Serbia | | | | | | |
| Shanghai Cooperation Organization | | | | | | |
| South Africa | | | | | | |
| South Korea | | | | | | |
| Spain | | | | | | |
| Sweden | | | | | | |
| Switzerland | | | | | | |
| Turkey | | | | | | |
| Uganda | | | | | | |
| Ukraine | | | | | | |
| United Kingdom | | | | | | |
| United States of America | 1 | | 2 | 3 | 2 | 2 |
| Venezuela | | | | | | |

## XII. Number of Citations by Term and Source – Others – Part 2/3

| Source | Cyber Attack | Cyber Conflict | Cyber Defense | Cyber Infrastructure Resilience | Cyber Operations | Cyber Threat | Cyberspace Operations |
|---|---|---|---|---|---|---|---|
| **Total** | 15 | 1 | 6 | 1 | 4 | 8 | 1 |
| African Union | | | | | | | |
| Armenia | | | | | | | |
| Australia | | | | | | | |
| Austria | 1 | | 1 | | | | |
| Azerbaijan | | | | | | | |
| Belarus | | | | | | | |
| Belgium | | | | | | | |
| Bolivia | | | | | | | |
| Brunei | | | | | | | |
| Canada | 1 | | | | | | |
| China | | | | | | | |
| Colombia | 1 | | 1 | | | | |
| Commonwealth of Independent States | | | | | | | |
| Council of Europe | | | | | | | |
| Cuba | | | | | | | |
| Czech Republic | 1 | | | | | | |
| Denmark | | | | | | | |
| EastWest Institute | 1 | 1 | 1 | | 1 | 1 | |
| Economic Community of West African States | | | | | | | |
| Ecuador | | | | | | | |
| Estonia | | | | | | 1 | |
| European Union | | | | | | | |
| Finland | | | | | | 1 | |
| France | | | 1 | | | | |
| Georgia | | | | | | 1 | |
| Germany | 2 | | | | | 1 | |
| Ghana | | | | | | | |
| Hungary | | | | | | | |
| India | | | | | | | |
| Institute of Electrical and Electronic Engineers | | | | | | | |
| International Organization for Standardization | | | | | | | |
| International Telecommunication Union | | | | | | | |
| Internet Engineering Task Force | | | | | | | |
| Internet Society | | | | | | | |
| Israel | | | | | | | |
| Italy | | | | | | 1 | |
| Japan | | | | | | | |
| Jordan | | | | | | | |
| Kazakhstan | | | | | | | |
| Kenya | | | | | | | |
| Latvia | | | | | | | |

| Source | Cyber Attack | Cyber Conflict | Cyber Defense | Cyber Infrastructure Resilience | Cyber Operations | Cyber Threat | Cyberspace Operations |
|---|---|---|---|---|---|---|---|
| League of Arab States | | | | | | | |
| Lebanon | | | | | | | |
| Lithuania | | | | | | | |
| Mali | | | | | | | |
| Mongolia | | | | | | | |
| Montenegro | | | | | | | |
| Netherlands | | | | | | | |
| New Zealand | 1 | | | | | | |
| North Atlantic Treaty Organization | 1 | | 1 | | 1 | | |
| Norway | | | | | | | |
| Oman | | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | | |
| Oxford Dictionary of Computing (2004) | | | | | | | |
| Oxford Dictionary of Computing (2008) | | | | | | | |
| Oxford English Dictionary | 1 | | | | | 1 | |
| Panama | | | | | | | |
| Philippines | | | | | | | |
| Poland | | | | | | | |
| Qatar | | | | | | | |
| Romania | 1 | | 1 | 1 | | 1 | |
| Russia | | | | | | | |
| Saudi Arabia | | | | | | | |
| Serbia | | | | | | | |
| Shanghai Cooperation Organization | | | | | | | |
| South Africa | | | | | | | |
| South Korea | | | | | | | |
| Spain | | | | | | | |
| Sweden | | | | | | | |
| Switzerland | 1 | | | | | | |
| Turkey | | | | | | | |
| Uganda | | | | | | | |
| Ukraine | | | | | | | |
| United Kingdom | 1 | | | | | | |
| United States of America | 2 | | | | 2 | | 1 |
| Venezuela | | | | | | | |

## XIII. Number of Citations by Term and Source – Others – Part 3/3

| Source | Exploit | Hacker | Hacking | Hacktivism | Information Assurance | Information Operations | Information Threat | Intruder | Intrusion | Malware | Threat |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Total** | 3 | 5 | 4 | 2 | 5 | 3 | 1 | 2 | 4 | 8 | 9 |
| African Union | | | | | | | | | | | |
| Armenia | | | | | | | | | | | |
| Australia | | | | | | | | | | | |
| Austria | | | | | | | | | | | |
| Azerbaijan | | | | | | | | | | | |
| Belarus | | | | | | | | | | | |
| Belgium | | 1 | | | | | | | | | |
| Bolivia | | | | | | | | | | | |
| Brunei | | | | | | | | | | | |
| Canada | | | | | | | | | | | |
| China | | | | | | | | | | | |
| Colombia | | | | | | | 1 | | | | 1 |
| Commonwealth of Independent States | | | | | | | | | | 1 | |
| Council of Europe | | | | | | | | | | | |
| Cuba | | | | | | | | | | | |
| Czech Republic | | | | | | | | | | | |
| Denmark | | | | | | | | | | | |
| EastWest Institute | | | | | | 1 | | | | | |
| Economic Community of West African States | | | | | | | | | | | |
| Ecuador | | | | | | | | | | | |
| Estonia | | | | | | | | | | | |
| European Union | | | | | | | | | | | |
| Finland | | | | | | | | | | | |
| France | | | | | | | | | | | |
| Georgia | | | | | | | | | | | |
| Germany | 1 | | 1 | 1 | | | | | | 2 | 1 |
| Ghana | | | | | | | | | | | |
| Hungary | | | | | | | | | | | |
| India | | | | | | | | | | | |
| Institute of Electrical and Electronic Engineers | | | | | | | | | | | |
| International Organization for Standardization | 1 | | 1 | 1 | | | | 1 | 1 | 1 | |
| International Telecommunication Union | | | 1 | | | | | | | 1 | 3 |
| Internet Engineering Task Force | | 1 | | | 1 | | | 1 | 1 | 1 | 1 |
| Internet Society | | | | | | | | | | | |
| Israel | | | | | | | | | | | |
| Italy | | | | | | | | | | | |
| Japan | | | | | | | | | | | |
| Jordan | | | | | 1 | | | | | | |
| Kazakhstan | | | | | | | | | | | |

| Source | Exploit | Hacker | Hacking | Hacktivism | Information Assurance | Information Operations | Information Threat | Intruder | Intrusion | Malware | Threat |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Kenya | | | | | | | | | | | |
| Latvia | | | | | | | | | | | |
| League of Arab States | | | | | | | | | | | |
| Lebanon | | | | | | | | | | | |
| Lithuania | | | | | | 1 | | | | | |
| Mali | | | | | | | | | | | |
| Mongolia | | | | | | | | | | | |
| Montenegro | | | | | | | | | | | |
| Netherlands | | | | | | | | | | | |
| New Zealand | | | | | | | | | | | |
| North Atlantic Treaty Organization | | | | | | | | | | | |
| Norway | | | | | | | | | | | |
| Oman | | | | | | | | | | | |
| Organization for Economic Cooperation and Development | | | | | | | | | | | |
| Organization for Security and Cooperation in Europe | | | | | | | | | | | |
| Oxford Dictionary of Computing (2004) | | 1 | 1 | | | | | | | | 1 |
| Oxford Dictionary of Computing (2008) | | | | | | | | | | | |
| Oxford English Dictionary | | | | | | | | | | | |
| Panama | | | | | | | | | | | |
| Philippines | | | | | | | | | | | |
| Poland | | | | | | | | | | | |
| Qatar | | | | | | | | | | | |
| Romania | | | | | | | | | | | |
| Russia | | | | | | | | | | | |
| Saudi Arabia | | | | | | | | | | | |
| Serbia | | | | | | | | | | | |
| Shanghai Cooperation Organization | | | | | | | | | | | |
| South Africa | | | | | | | | | | | |
| South Korea | | | | | | | | | | | |
| Spain | | | | | | | | | | | |
| Sweden | | | | | | | | | | | |
| Switzerland | | | | | | | | | | | |
| Turkey | | | | | | | | | | | |
| Uganda | | | | | | | | | | | |
| Ukraine | | | | | | | | | | | |
| United Kingdom | | | | | | | | | | | |
| United States of America | 1 | 2 | | | 3 | 1 | | | 2 | 2 | 2 |
| Venezuela | | | | | | | | | | | |

## XIV. Total Number of Citations by Source Type

| Term | State - P5 | State - UNGGE4 | State - OSCE | State – Other | IGO | Other Source | Total |
|---|---|---|---|---|---|---|---|
| Total | 103 | 61 | 104 | 48 | 38 | 92 | 446 |
| Attack | 1 | 1 | | | 2 | 3 | 7 |
| Attacker | | | | | | 3 | 3 |
| Computer | | | | 1 | | 1 | 2 |
| Computer Network Attack | 2 | | 1 | | 1 | | 4 |
| Computer Network Defense | 3 | | 1 | | | | 4 |
| Computer Network Exploitation | 2 | | 1 | | | | 3 |
| Computer Network Operations | 2 | | 3 | | | | 5 |
| Computer Security | 2 | | | | | 3 | 5 |
| Computer System | | | | | 1 | 1 | 2 |
| Critical | | | | | | 2 | 2 |
| Critical ICT Infrastructure | | | 1 | | | | 1 |
| Critical Information Infrastructure | 1 | | 2 | | | 1 | 4 |
| Critical Infrastructure | 5 | 3 | 6 | 2 | | 1 | 18 |
| Critical Infrastructure and Key Resources | 1 | | | | | | 1 |
| Critical National Infrastructure | | | | 1 | | | 1 |
| Cyber Attack | 3 | 3 | 5 | 1 | | 3 | 15 |
| Cyber Conflict | | | | | | 1 | 1 |
| Cyber Crimes or Information Crimes | | | | 1 | | | 1 |
| Cyber Defense | 1 | 1 | 2 | | | 3 | 7 |
| Cyber Domain | | | 1 | | | | 1 |
| Cyber Environment | | | | | 1 | | 1 |
| Cyber Espionage | 1 | 1 | 3 | 1 | | 3 | 9 |
| Cyber Incident | 2 | | 3 | 1 | | | 6 |
| Cyber Infrastructure | 2 | | | | | 1 | 3 |
| Cyber Infrastructure Resilience | | | 1 | | | | 1 |
| Cyber Operations | 2 | | | | | 2 | 4 |
| Cyber Sabotage | | 1 | 1 | | | | 2 |
| Cyber Space | 10 | 10 | 14 | 5 | 1 | 5 | 45 |
| Cyber Terrorism | | 2 | 6 | | 1 | 2 | 11 |
| Cyber Threat | | 2 | 4 | | | 2 | 8 |
| Cyber War | | | 3 | | | 4 | 7 |
| Cyber Warfare | | | 1 | 1 | | 1 | 3 |
| Cyber Weapon | | | | | | 2 | 2 |
| Cybercrime | 2 | 5 | 4 | 5 | 1 | 3 | 20 |
| Cybersecurity | 9 | 9 | 16 | 6 | 3 | 6 | 49 |
| Cyberspace Operations | 1 | | | | | | 1 |
| Electronic Information Infrastructure | | | 1 | | | | 1 |
| Exploit | 1 | 1 | | | | 1 | 3 |
| Global Information Infrastructure | | | | | 1 | | 1 |
| Hacker | 2 | | 1 | | | 2 | 5 |
| Hacking | | 1 | | | 1 | 2 | 4 |
| Hacktivism | | 1 | | | | 1 | 2 |

| Term | P5 | UNGGE4 | OSCE | Other State | IGO | Other Source | Total |
|---|---|---|---|---|---|---|---|
| ICT Infrastructure | | | 1 | | | | 1 |
| Information | 2 | | 1 | 2 | 2 | 4 | 12 |
| Information and Communication Technologies | 1 | 2 | 1 | 1 | 1 | | 6 |
| Information and Communication Networks (ICN) Security Incident | | | | | 1 | | 1 |
| Information Area | 1 | | | | | | 1 |
| Information Assurance | 3 | | | 1 | | 1 | 5 |
| Information Crime | | | 1 | | | | 1 |
| Information Environment | 1 | | 1 | | | | 2 |
| Information Incident | | 1 | | | | | 1 |
| Information Infrastructure | 1 | 1 | | | | | 2 |
| Information Operations | 1 | | 1 | | | 1 | 3 |
| Information Security | 10 | 4 | 8 | 8 | | 3 | 33 |
| Information Security Event | | | | | | 2 | 2 |
| Information Security Incident | | | | | | 3 | 3 |
| Information Space | 2 | | | | | 2 | 4 |
| Information Sphere | 1 | | | 1 | | | 2 |
| Information System | 3 | 1 | 4 | | 3 | 3 | 14 |
| Information System Security | 1 | | | | | | 1 |
| Information Technologies Security Incident | | | 1 | | | | 1 |
| Information Technology | 2 | 2 | 1 | 1 | 1 | 1 | 8 |
| Information Technology and Communications | | | | | 1 | | 1 |
| Information Terrorism | | | | 1 | 1 | | 2 |
| Information Threat | | 1 | | | | | |
| Information War | 3 | | | | | 1 | 4 |
| Information Warfare | | | | 2 | | | 2 |
| Information Weapon | 3 | | | 3 | | | 6 |
| International Information Security | 1 | | | 1 | | | 2 |
| International Information Terrorism | 1 | | | | | | 1 |
| Internet Crime | | | | | | 1 | 1 |
| Internet Security | | | 1 | | | | 1 |
| Intruder | | | | | | 2 | 2 |
| Intrusion | 2 | | | | | 2 | 4 |
| IT Security | | 3 | | | | | 3 |
| Malware | 2 | 2 | | | 2 | 2 | 8 |
| National Critical Infrastructure and Key Assets | 1 | | | | | | 1 |
| Security | 1 | | | | 3 | 4 | 8 |
| Security Incident | | | | | 2 | 1 | 3 |
| Security of Information | | | 1 | 1 | | | 2 |
| the Internet | 1 | 1 | | | 1 | 3 | 6 |
| Threat | 2 | 2 | | | 3 | 2 | 9 |
| Use of the Internet as a Weapon | | | 1 | | | | 1 |
| Use of the Internet for Terrorist Purposes | | | | 1 | | | 1 |
| Vital Structures | 2 | | | | | | 2 |

# WORKS CITED


African Union, African Union Commission, "Draft African Union Convention on the Establishment of a credible legal Framework for Cyber Security in Africa," African Union Commission, 2011.<http://au.int/en/cyberlegislation >

Armenia, Submission to the United Nations General Assembly Resolution A/68/156/Add.1, 2013. <https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/e68ed4bd170321b285257bc70067f864/$FILE/A%2068%20156%20Add1.pdf >

Australia, Submission to the United Nations General Assembly Resolution A/54/213, 1999. <https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf >

Australia, Australian Government, "Cyber Security Strategy," Commonwealth of Australia, 2009. <http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx >

Austria, Bundeskanzleramt Osterreich, "Austrian Cyber Security Strategy," Federal Chancellery of the Republic of Austria, 2013. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world >

Austria, Digital Austria, "National ICT Security Strategy Austria," Federal Chancellery of the Republic of Austria, 2012. <http://www.enisa.europa.eu/media/news-items/new-cyber-security-strategies-of-austria-finland-worldwide >

Azerbaijan, The Republic of Azerbaijan, "Law on Information, Informatisation and Protection of Information," The Law of the Republic of Azerbaijan, 1998. <https://www.ecoi.net/azerbaijan/nationallaw >

Belarus, Department of the Interior (Министерство Внутренних Дел Рецпублики Беларусъ), Концепция Националъной Безопасности (Concept of National Security of the Republic of Belarus), Department of the Interior (Министерство Внутренних Дел Рецпублики Беларусъ), 2010. <http://mvd.gov.by/ru/main.aspx?guid=14961 >

Belarus, Council of Ministers of the Republic of Belarus, "Law of the Republic of Belarus 'On Information, Informatization and Protection of information'," Council of Ministers of the Republic of Belarus, 2008. <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan042125.pdf >

Belgium, Government of Belgium. "Cyber Security Strategy," Government of Belgium, 2012. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world >

Bolivia, Submission to the United Nations General Assembly Resolution A/58/373, 2003. <https://disarmament-library.un.org/UNODA/Library.nsf/c793d171848bac2b85256d7500700384/b69c21ea9dcbb95785256dc10058b4c9/$FILE/sg58.373.pdf >

Brunei Darussalam, Submission to the United Nations General Assembly Resolution A/62/98, 2008. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/62/98 >

Canada, Submission to the United Nations General Assembly Resolution A/60/95/Add.1, 2005. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/518/77/PDF/N0551877.pdf?OpenElement >

Canada, Government of Canada, "Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada," Her Majesty the Queen in Right of Canada, 2010. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx >

China, Submission to the United Nations General Assembly Resolution A/61/161, 2006. <https://disarmament-library.un.org/UNODA/Library.nsf/df4241a26771ddbd852571a8006cd413/8cc65546257a1692852571cb00566c6e/$FILE/sg61.161.pdf >

China, Submission to the United Nations General Assembly Resolution A/62/98, 2008. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/62/98 >

Colombia, Departmento Nacional de Planeacion, "Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de política para la Ciberseguridad y Ciberdefensa)," Consejo Nacional de Politica Economica y Social, 2011. <http://www.mintic.gov.co/portal/604/w3-article-3510.html >

Commonwealth of Independent States, Member States "Agreement on cooperation among states in combating offences relating to computer information," Commonwealth of Independent States, 2001. <https://cms.unov.org/documentrepositoryindexer/GetDocInOriginalFormat.drsx?DocID=5b7de69a-730e-43ce-9623-9a103f5cabc0 >

Council of Europe, Convention Committee on Cybercrime, "Convention on Cybercrime," The Council of the European Union, 2001. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

Council of Europe, The Council of the European Union. "Council Framework Decision 2005/222/JHA of February 2005 on attacks against information systems," The Council of the European Union, 2005. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN >

Cuba, Submission to the United Nations General Assembly Resolution A/54/213, 1999. <https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf >

Cuba, Submission to the United Nations General Assembly Resolution A/57/166/Add.1, 2002. <https://disarmament-library.un.org/UNODA/Library.nsf/711f8f7e30e9272785256beb004f8126/742141d7cf13d74b85256c0e0052e5ae/$FILE/sg57.166a.pdf >

Cuba, Submission to the United Nations General Assembly Resolution A/58/373, 2003. <https://disarmament-library.un.org/UNODA/Library.nsf/c793d171848bac2b85256d7500700384/b69c21ea9dcbb95785256dc10058b4c9/$FILE/sg58.373.pdf >

Czech Republic, Government of the Czech Republic, "Cyber Security Strategy of the Czech Republic for the 2011-2015 Period," Government of the Czech Republic, 2011. <http://www.enisa.europa.eu/media/news-items/czech-cyber-security-strategy-published >

Czech Republic, Parliament of the Czech Republic, "Draft Act on Cyber Security," Government of the Czech Republic, 2014. <http://www.govcert.cz/download/nodeid-1246/ >

Denmark, The Danish Parliament, “Danish Defence Agreement 2010-2014,” Government of Denmark, 2009. <http://www.fmn.dk/eng/allabout/Pages/Prior-Danish-Defence-Agreements.aspx >

EastWest Institute. James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko. "Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2, Issue 2." The EastWest Institute, 2011. <http://www.ewi.info/idea/critical-terminology-foundations-2>

Economic Community of West African States, Council of Ministers, “Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS.” ECOWAS, 2011. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fwww.ecowas.int%2Fpublications%2Fen%2Factes_add_telecoms%2FSIGNED-Cybercrime.pdf&ei=svwuVMDLJauHsQTWtoDoBQ&usg=AFQjCNFaJK43Y-SzuSD8cS96qJbtEOzSng&sig2=UuQQVFZ4bq0-tz9nUO2n9Q&bvm=bv.76802529,d.cWc >

Ecuador, Submission to the United Nations General Assembly Resolution A66/152/Add.1

Estonia, Cyber Security Strategy Committee, “Cyber Security Strategy,” Ministry of Defence, 2008. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world >

European Union, High Representative of the European Union for Foreign Affairs and Security Policy, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2013. <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security >

Finland, Secretariat of the Security and Defence Committee, “Finland’s Cyber Security Strategy,” Ministry of Defence, 2013. <http://www.enisa.europa.eu/media/news-items/new-cyber-security-strategies-of-austria-finland-worldwide >

France, Agence Nationale de la Securite des Systemes d’Information, “Information Systems Defence and Security: France’s Strategy, Republique Francaise, 2011. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world >

Georgia, Government of Georgia. “National Security Concept of Georgia,” Government of Georgia, 2011. <http://www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=12 >

Germany, Submission to the United Nations General Assembly Resolution A/66/152, 2011. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/416/91/PDF/N1141691.pdf?OpenElement >

Germany, Submission to the United Nations General Assembly Resolution A/68/156, 2013. <https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/e68ed4bd170321b285257bc70067f864/$FILE/A%2068%20156.pdf >

Germany, Government of Germany, “Cyber Security Strategy for Germany,” Government of Germany, 2011. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world >

Germany, Department of the Interior, “Implementation Plan KRITIS,” Government of Germany, 2007. <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf?__blob=publicationFile>

Germany, Federal Criminal Police Office, “Federal Overview Cybercrime 2013,” Federal Criminal Police Office, 2013. <http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2012,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2012.pdf >

Germany, Federal Office for Information Security (BSI), “Cybersecurity,” Bundesmat fur Sicherheit in der Informationstechnik, 2014. <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html >

Germany, Federal Office for Information Security (BSI), „Glossary/Terminology,“ Bundesmat fur Sicherheit in der Informationstechnik, 2014. <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Glossar/cs_Glossar_A.html;jsessionid=C8733A22C9EABECEC04B7FDDDE34C451.2_cid294 >

Ghana, William Tevie, “Making our Cyber Space Safe,” National IT Agency of Ghana, 2014. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.isaca.org%2Fchapters9%2FAccra%2FEvents%2FDocuments%2FMaking%2520our%2520cyber%2520Space%2520Safe.pdf&ei=XQEvVOXKKvb9sASxm4KwCA&usg=AFQjCNHB4pP0ECWrm7RBPsSUu28otqzhIQ&sig2=A6E6kR1B_4X7z15eBhOpNg&bvm=bv.76802529,d.cWc >

Hungary, National Security Authority, “Act L of 2013 on Electronic Information Security of Central and Local Government Agencies,” Government of Hungary, 2013. <http://www.nbf.hu/legis.html >

Hungary, Government of Hungary, “Annex 1 to Government Decision No. 1139/2013 National Cyber Security Strategy of Hungary,” Government of Hungary, 2013. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world >

India, Ministry of Communication and Information Technology and the Department of Electronics and Information Technology, “National Cyber Security Policy – 2013 (NCSP-2013),” Government of India, 2013. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world >

India, Ministry of Law, Justice and Company Affairs, “The Information Technology Act, 2008,” Government of India, 2008. <http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf >

Institute of Electrical and Electronic Engineers, “IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems – ‘Information’,” IEEE, 2007.
[Information] <http://dictionary.ieee.org/index/i-5.html >

Institute for Electronic and Electrical Engineers, “IEEE Recommended for Practice for Futurebus+,” IEEE, 1993.
[Computer Security] <http://dictionary.ieee.org/index/c-12.html >

Institute for Electronic and Electrical Engineers, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations – ‘Cyber Security,’ ‘Computer Security’,” IEEE, 2010. [Cyber Security] <http://dictionary.ieee.org/index/c-21.html >
[Computer Security] <http://dictionary.ieee.org/index/c-12.html >

International Organization for Standardization, “ISO/IEC Glossary of IT Security Terminology,” ISO/IEC, 2013. <http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=64540&languageid=en&cmsareaid=64540 >

Applies to all ITU terms except for cybersecurity, hacking, information security incident, malware, information technology:
International Telecommunication Union, “ITU Terms and Definitions,” Updated 2014, <http://www.itu.int/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en&adsearch=&SearchTerminology=exploit&collection=both&sector=all&language=all&part=abbreviationterm&kind=anywhere&StartRecord=1&NumberRecords=50 >

Applies only to the following ITU terms: cybersecurity, hacking, information security incident, malware, information technology:
International Telecommunication Union, “Termite 6L – Terminology of Telecommunications – V.7,” Updated 2014. <http://www.itu.int/online/termite/index.html >

Internet Engineering Task Force, “Internet Security Glossary Version 2,” The IETF Trust, 2007. <http://tools.ietf.org/html/rfc4949 >

Internet Society, “Some Perspectives on Cybersecurity: 2012,” Internet Society, 2012. <http://www.internetsociety.org/doc/some-perspectives-cybersecurity-2012 >

Israel, Government of Israel, “Resolution No. 3611: Advancing National Cyberspace Capabilities,” Government of Israel, 2011. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA&url=http%3A%2F%2Fwww.pmo.gov.il%2FEnglish%2FPrimeMinistersOffice%2FDivisionsAndAuthorities%2Fcyber%2FDocuments%2FAdvancing%2520National%2520Cyberspace%2520Capabilities.pdf&ei=9QwvVK2ICuHksAT2n4DgCA&usg=AFQjCNF48_baBX5K4dW5RIrQLH_lHLhnmw&sig2=3dmMF2sDvwjAp1VkMH7jjQ&bvm=bv.76802529,d.cWc >

Italy, Presidency of the Council of Ministers, “National Strategic Framework for Cyberspace Security, Government of Italy,” 2013. <https://www.ccdcoe.org/strategies-policies.html >

Japan, Information Security Policy Council, “Cybersecurity Strategy: Towards a World-leading, Resilient and Vigorous Cyberspace,” Government of Japan, 2013. <http://www.nisc.go.jp/eng/ >

Japan, Government of Japan, “National Security Strategy” Government of Japan, 2013. <http://www.cas.go.jp/jp/siryou/ >

Japan, Information Security Policy Council, “The First National Strategy on Information Security,” Government of Japan, 2006. <www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf >

Japan, Information Security Policy Council, "The Second National Strategy on Information Security," Government of Japan, 2009. <www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf >

Jordan, Submission to the United Nations General Assembly Resolution A/61/161, 2006. <https://disarmament-library.un.org/UNODA/Library.nsf/df4241a26771ddbd852571a8006cd413/8cc65546257a1692852571cb00566c6e/$FILE/sg61.161.pdf >

Jordan, Ministry of Information and Communications Technology, "National Information Assurance and Cyber Security Strategy (NIACSS)," Government of Jordan, 2012. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjAA&url=http%3A%2F%2Fnitc.gov.jo%2FPDF%2FNIACSS.pdf&ei=XhEvVNfvKrSAsQTl_oKgDQ&usg=AFQjCNFE5e5p0ncoWB9u38U3J6d-9efSjg&sig2=IQPx8lVZyMP2lFQpAgtCWg&bvm=bv.76802529,d.cWc >

Kazakhstan, Submission to the United Nations General Assembly Resolution A/64/129, 2009. <https://disarmament-library.un.org/UNODA/Library.nsf/aeca18509aa92c5c852575610076cc98/76c7a108d32a1402852576080048205b/$FILE/A-64-129.pdf >

Kenya, Ministry of Information Communications and Technology, "Cybersecurity Strategy," Government of Kenya, 2014. <https://www.ccdcoe.org/strategies-policies.html >

Latvia, Government of Latvia, "Law on Security of Information Technologies," Government of Latvia, 2012. <https://www.ccdcoe.org/strategies-policies.html >

League of Arab States, General Secretariat, "Arab Convention on Combating Information Technology Offenses," League of Arab States, 2010. <https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd >

Lebanon, Submission to the United Nations General Assembly Resolution A/62/98, 2007, <https://disarmament-library.un.org/UNODA/Library.nsf/e5e236cc645fcd048525731d006514e5/eb8151fef5a2f1ec85257328004c4bf4/$FILE/a-62-98.pdf >

Lithuania, Government of the Republic of Lithuania, "Resolution No. 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019," Government of the Republic of Lithuania, 2011. <http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf >

Lithuania, Lithuanian Armed Forces, "Lithuanian Military Doctrine," Information Provision Service of the General Affairs Department of the Ministry of National Defence, 2010. <http://kariuomene.kam.lt/en/military_insignia/lithuanian_military_doctrine.html >

Lithuania, Government of the Republic of Lithuania, "Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019," Government of the Republic of Lithuania, 2011. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/programme-for-the-development-of-electronic-information-security-cyber-security-for-2011-2019-2011 >

Mali, Submission to the United Nations General Assembly Resolution A/64/129/Add.1, 2009. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/505/75/PDF/N0950575.pdf?OpenElement>

Mongolia, Government of Mongolia, The Concept of National Security of Mongolia, Government of Mongolia. <http://www.nsc.gov.mn/sites/default/files/images/National%20Security%20Concept%20of%20Mongolia%20EN.pdf >

Montenegro, Ministry of Defense, "National Cyber Security Strategy for Montenegro 2013-2017," Ministry of Defense, 2013. <http://webcache.googleusercontent.com/search?q=cache:IEnxtD9e4WUJ:www.mid.gov.me/ResourceManager/FileDownload.aspx%3Frid%3D165416%26rType%3D2%26file%3DCyber%2520Security%2520Strategy%2520for%2520Montenegro.pdf+&cd=1&hl=en&ct=clnk&gl=us >

North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence, Schmitt, Michael N., "The Tallinn Manual on International Law Applicable to Cyber Warfare," NATO Cooperative Cyber Defence Center of Excellence, 2013. <http://www.ccdcoe.org/tallinn-manual.html >

Netherlands, Ministry of Security and Justice, "National Cyber Security Strategy 2: From awareness to capability," Ministry of Security and Justice, 2013. <http://webcache.googleusercontent.com/search?q=cache:1x0f8GWV_T4J:https://english.nctv.nl/Images/national-cyber-security-strategy-2_tcm92-520278.pdf+&cd=1&hl=en&ct=clnk&gl=us >

Netherlands, Ministry of Defence, "The Defence Cyber Strategy," Netherlands Ministry of Defence, 2012. <http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf >

New Zealand, Ministry for Communications and Information Technology, "New Zealand's Cyber Security Strategy," Ministry for Communications and Information Technology, 2011. <http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf >

Norway, Norwegian Ministries, "Cyber Security Strategy for Norway," Government of Norway, 2012. <http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf >

Sommer, Peter and Ian Brown, "Reducing Systemic Cybersecurity Risk," OECD/IFP Project on "Future Global Shocks", 2011. <http://www.oecd.org/governance/risk/46889922.pdf >

Oman, Submission to the United Nations General Assembly Resolution A/54/213, 1999. <https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf >

Organization for Security and Co-Operation in Europe, Action against Terrorism Unit, "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace," Transnational Threats Department, 2013. <http://www.osce.org/atu/103500?download=true >

The Oxford English Dictionary, 2014

Oxford University, Oxford University Press, "A Dictionary of Computing," Oxford University Press, 2004.

Oxford University, Daintith, John and Edumnd Wright, "A Dictionary of Computing," Oxford University Press, 2008.

Panama, Submission to the United Nations General Assembly Resolution A/65/154, 2010. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/458/42/PDF/N1045842.pdf?OpenElement>

Philippines, Submission to the United Nations General Assembly Resolution A/56/164, 2001. <http://www.un.org/documents/ga/docs/56/a56164.pdf>

Poland, Ministry of Administration and Digitisation, Internal Security Agency, "Cyberspace Protection Policy of the Republic of Poland," Ministry of Administration and Digitisation, Internal Security Agency, 2013. <http://webcache.googleusercontent.com/search?q=cache:AdaO5iVXAXcJ:www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf+&cd=1&hl=en&ct=clnk&gl=us >

Qatar, Submission to the United Nations General Assembly Resolution A/54/213, 1999. <https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf >

Romania, CERT Romania, "Resolution no . 271/2013 approving Romania's cyber security strategy and national action plan on implementation of the national cybersecurity (Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică)," CERT Romania, 2013. <http://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf >

Russia, Submission to the United Nations General Assembly Resolution A/54/213, 1999. <https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf >

Russia, Submission to the United Nations General Assembly Resolution A/55/140, 2000. <http://www.un.org/documents/ga/docs/55/a55140.pdf >

Russia, Russian Federation, "Concept Strategy for Cybersecurity of the Russian Federation (Концепция Стратегии Кибербезопасности Проссийской Федерации)," Russian Federation. <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf >

Russia, Ministry of Defense (Министерство Обороны) "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве)," Ministry of Defense, 2011. <http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle >

Russia, Ministry of Foreign Affairs (Министрество Иностранных Дел), Information Security Doctrine of the Russian Federation, Ministry of Foreign Affairs, 2000. <http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument >

Saudi Arabia, Ministry of Communication and Information Technology, Developing National Information Security Strategy for the Kingdom of Saudi Arabia NISS, Draft 7, Ministry of Communication and Information Technology, 2013. <http://www.mcit.gov.sa/Ar/MediaCenter/PubReqDocuments/NISS_Draft_7_EN.pdf >

Shanghai Cooperation Organization, Chinese, Russian, Tajik, and Uzbek representatives to the United Nations General Secretary, "Annex to the letter dated 12 September 2011 from the Permanent

Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary General: International code of conduct for information security, 2011. <http://content.netmundial.br/files/67.pdf >

Serbia, General Secretariat, «Стратегију развоја информационог друштва у Републици Србији до 2020. Године,» Serbian Government, 2011. <http://www.gs.gov.rs/english/strategije-vs.html >

South Africa, Department of Communications, "Notice of Intention to make South African National Cybersecurity Policy," Department of Communications, 2010. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/southafricancss.pdf >

South Africa, Department: Defence Republic of South Africa, "South African Defence Review 2012," 2012. <http://www.gov.za/documents/detail.php?cid=335418 >

South Korea, South Korean Ministry of Defense, "2012 Defense White Paper," South Korean Ministry of Defense, 2012. <http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_20130814005219260.pdf >

Spain, Submission to the United Nations Resolution A/64/129/Add.1, 2009. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/505/75/PDF/N0950575.pdf?OpenElement >

Spain, Departmento De Seguridad Nacional, "National Cyber Security Strategy," Presidencia Del Gobierno, 2013. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf >

Sweden, Submission to the United Nations General Assembly Resolution A/68/243, 2014. <https://gafc-vote.un.org/UNODA/vote.nsf/511260f3bf6ae9c005256705006e0a5b/a996d3f46c2494e385257c520054d0ae/$FILE/A%20RES%2068%20243.pdf >

Switzerland, Federal Department of Defence, Civil Protection and Sport DDPS, "National strategy for the protection of Switzerland against cyber risks," Federal Department of Defence, Civil Protection and Sport DDPS, 2012. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf >

Turkey, Ministry of Transport, Maritime Affairs and Communications, "National Cyber Security Strategy and 2013-2014 Action Plan," Ministry of Transport, Maritime Affairs and Communications, 2013. <http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf >

Uganda, Ministry of Information and Communications Technology, "National Information Security Strategy," Ministry of Information and Communications Technology, 2011. <http://www.sicurezzacibernetica.it/en/[Uganda]%20National%20Cyber%20Security%20Strategy%20-%202011%20-%20EN.pdf >

Ukraine, Submission to the United Nations General Assembly Resolution A/58/373, 2003. <https://disarmament-library.un.org/UNODA/Library.nsf/c793d171848bac2b85256d7500700384/b69c21ea9dcbb95785256dc10058b4c9/$FILE/sg58.373.pdf >

Ukraine, Submission to the United Nations General Assembly Resolution A/68/156, 2013. <https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/e68ed4bd170321b285257bc70067f864/$FILE/A%2068%20156.pdf >

United Kingdom, Submission to the United Nations General Assembly Resolution A/54/213, 1999. < https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf >

United Kingdom, Submission to the United Nations General Assembly Resolution A/68/156, 2013. < https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/e68ed4bd170321b285257bc70067f864/$FILE/A%2068%20156.pdf>

United Kingdom, UK Cabinet Office, "Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space," UK Cabinet Office, 2009. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf >

United Kingdom, Parliamentary Office of Science & Technology, "POSTnote Number 389: Cyber Security in the UK," UK House of Parliament, 2011. <http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf >

United Kingdom, UK Cabinet Office, "The Cost of Cyber Crime," UK Cabinet Office, 2011. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf >

United Kingdom, UK Cabinet Office, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world," UK Cabinet Office, 2011. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf >

United States of America, The Army, "The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028," U.S. Department of Defense. 2010. <http://fas.org/irp/doddir/army/pam525-7-8.pdf>

United States of America, Committee on National Security Systems, "CNSS National Information Assurance Glossary," Committee on National Security Systems, 2010. <http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf >

United States of America, Office of the Press Secretary, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," The White House, 2009. <http://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees >

United States of America, U.S. Joint Chiefs of Staff, "Department of Defense Dictionary of Military and Associated Terms," U.S. Joint Chiefs of Staff, 2010 (As Amended Through 15 August 2014). <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf >

United States of America, Office of the Press Secretary, "Executive Order -Improving Critical Infrastructure Cybersecurity," The White House, 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity >

United States of America, National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” U.S. Department of Commerce, 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf >

United States of America, U.S. Joint Chiefs of Staff, “Information Operations Joint Publication 3-13,” U.S. Joint Chiefs of Staff, 2006. <http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf >

United States of America, National Initiative for Cybersecurity Careers and Studies, “Explore Terms: A Glossary of Common Cybersecurity Terminology,” U.S. Department of Homeland Security. <http://niccs.us-cert.gov/glossary >

United States of America, Kissel, Richard, “National Institute of Standards and Technology Glossary of Key Information Security Terms,” U.S. Department of Commerce, 2013. <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf >

United States of America, The White House, “The National Strategy to Secure Cyberspace,” The White House, 2003. <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf >

Venezuela, Submission to the United Nations General Assembly Resolution A/59/116/Add.1, 2004. < https://disarmament-library.un.org/UNODA/Library.nsf/67458ce237aeef6785256ebd004bfee8/d5fc7c844390a5f885256ef9004ce0a3/$FILE/sg59.116a1.pdf >

[i] Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.
[ii] Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung oder Ubertragung von Informationen.
[iii] Globales Computer-Netz (Netz der Netze), basierend auf dem Übertragungsstandard (Protokoll) TCP/IP. Das Internet funktioniert plattform- und betriebssystemübergreifend. Typische Dienste im Internet sind World Wide Web (WWW) und E-Mail.
[iv] сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)
[v] Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
[vi] Le cyberespace est l'environment global ne de l'interconnexion des systemes d'information et de communication. Le cyberespace est plus large que le monde informatique et contient egalement les reseaux informatiques, systemes informatiques, medias et donnes numeriques, qu'ils soient physiques ou virtuels.
[vii] Spaţiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere, dar şi riscuri la adresa funcţionării acesteia.
[viii] Mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta.
[ix] сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.
[x] совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.
[xi] Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
[xii] Cyber-Sicherheit erweitert das Aktionsfeld der klassischen IT-Sicherheit auf den gesamten Cyber-Raum. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Damit wird praktisch die gesamte moderne Informations- und Kommunikationstechnik zu einem Teil des Cyber-Raums.
[xiii] La cybersecurite est la situation souhaitee ou la protection du cyberspace est proportionnelle a la cybermenace et aux consequences possibles de cyberattaques. Dans une situation de cybersecurite, la perturbation, l'attaque ou l'utilisation abusive de l'ICT ne provoque aucun danger ni dommage. Les consequences de l'abus, de la perturbation ou de l'attaque peuvent consister en la restriction de la disponibilte et de la fiabilte de l'ICT, en la violation de la confidentialite des informations ou en des dommages causes a l'integrite de ces informations (ajout, effacement ou modification illegaux).
[xiv] Starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. Măsurile proactive şi reactive pot include politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor.
[xv] информационная безопасность – состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.
[xvi] Состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.
[xvii] Информациона безбедност значи заштиту система, података и инфраструктуре у циљу очувања поверљивости, интегритета и расположивости информација.
[xviii] IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.
[xix] IT-Sicherheit ist der Zustand, in dem Verfuegbarkeit, Integritaet und Vertaulichkeit von Informationen und Informationstechnik duch angemesse Massnahmen geschuetzt sind.

[xx] Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfugbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1. In informationstechnischen Systemen, Komponenten oder Prozessen oder, 2. Bei der Anwendung von informationstechnischen System, Komponenten oder Prozessen.

[xxi] состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. Система обеспечения информационной безопасности.

[xxii] Eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează securitatea cibernetică.

[xxiii] Cualquier evento adverso real o sospechado en relación con la seguridad de sistemas de computación o redes de computación.

[xxiv] Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación.

[xxv] Совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации.

[xxvi] Die Gesamtheit der IT-Anteile einer Infrastruktur wird als deren Informationsinfrastruktur bezeichnet.

[xxvii] информационные технологии, средства и методы, применяемые в целях ведения.

[xxviii] Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia)

[xxix] Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)

[xxx] Cybercrime umfasst die Straftaten,
- Die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten,
- Die mittels dieser Informationstechnik begangen werden.

[xxxi] Kriminelle Aktivitäten wobei Dienste oder Anwendungen im Cyber-Raum genutzt werden zur Durchführung der Kriminalität oder Ziel der Kriminalität sind. Dabei kann der Cyber-Raum Ausgangspunkt, Ziel oder der Ort der Kriminalität sein.

[xxxii] Totalitatea faptelor prevăzute de legea penală sau de alte legi speciale care prezintă pericol social şi sunt săvârşite cu vinovăţie, prin intermediul ori asupra infrastructurilor cibernetice.

[xxxiii] Acţiuni desfăşurate în spaţiul cibernetic, cu scopul de a obţine neautorizat informaţii confidenţiale în interesul unei entităţi statale sau nonstatale.

[xxxiv] La convergencia del terrorismo y ciberespacio con el fin de atacar ilegalmente ordenadores, redes e información almacenada en ellos, incluye violencia contra personas o propiedades o, al menos, genera el miedo. Abarca asesinatos, explosiones, contaminación de aguas o grandes pérdidas económicas, entre otras acciones. (Dorothy Denningal, profesora de la Universidad de Georgetown.)

[xxxv] Activităţile premeditate desfăşurate în spaţiul cibernetic de către persoane, grupări sau organizaţii motivate politic, ideologic ori religios ce pot determina distrugeri materiale sau victime, de natură să determine panică ori teroare.

[xxxvi] L'utilisation de cybercapacités à une échelle suffisante, durant une période déterminée et à haut débit, en vue d'atteindre certains objectifs ou effets dans ou au travers du cyberespace, ces actions étant considérées comme une menace pour les intérêts nationaux de l'Etat visé.

[xxxvii] противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

[xxxviii] Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

[xxxix] Procesul complex de planificare, coordonare, sincronizare, armonizare şi desfăşurare a acţiunilor în spaţiul cibernetic pentru protecţia, controlul şi utilizarea reţelelor de calculatore în scopul obţinerii superiorităţii informaţionale, concomitent cu neutralizarea capabilităţilor adversarulu.

[xl] Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia)

[xli] Angriffe, die im Cyber-Raum durch Tools, Dienste oder Anwendungen im Cyber-Raum durchgeführt werden; dabei kann der Cyber-Raum sowohl Ausgangspunkt, Ziel oder der Ort des Angriffs sein.

[xlii] Acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică.
[xliii] Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.
[xliv] Acţiuni desfăşurate în spaţiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva ameninţărilor asupra infrastructurilor cibernetice specifice apărării naţionale.
[xlv] Capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate.
[xlvi] (realistische) Möglichkeit eines nicht gewollten Vorfalls, der in der Schädigung eines technischen Systems, eines Individuums oder einer Organisation liegt.
[xlvii] Circumstanţă sau eveniment care constituie un pericol potenţial la adresa securităţii cibernetice.
[xlviii] Ein Exploit (englisch to exploit "ausnutzen") ist eine systematische Möglichkeit, Schwachstellen, die bei der Entwicklung eines Programms nicht berücksichtigt wurde, auszunutzen. Dabei werden mit Hilfe von Befehlsfolgen Sicherheitslücken und Fehlfunktionen von Programmen (oder ganzen Systemen) benutzt, meist um sich Zugang zu Ressourcen zu verschaffen oder Systeme zu beeinträchtigen
[xlix] Un hacker, tout en sachant qu'il n'y est pas autorisé, accède à ou surfe dans un système informatique.
[l] Intendierter Zugang zu einem Computersystem ohne notwendige Autorisierung durch den Nutzer oder den Eigentümer
[li] "Hacking" mit einer politischen oder sozialen Absicht
[lii] La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Ministerio de Defensa de Colombia)
[liii] Computerprogramme, die entwickelt und eingesetzt werden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen (Schad-SW) Beispiel: Viren, Trojaner, Würmer
[liv] Schadprogramme im Sinne dieses Gestzes sind Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu loschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Ablaufe einzuwirken.
[lv] Violación potencial de la seguridad.
[lvi] Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen bedrohen kann, wodurch dem Besitzer der Informationen ein Schaden entsteht.