jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2020, VOL. 66, NO. 1, PP. 243–248
Manuscript received October 10, 2019; revised January, 2020. DOI: 10.24425/ijet.2020.131870

Cyber(in)security

Krzysztof Szczypiorski

***Abstract*—The purpose of this article is to present three theses – (1) a cultural one: cyberspace is an advanced technical and cultural creation – it is an embodiment of dreams of numerous creators, inventors and engineers; (2) a technical one: security and cyberspace are inseparable components (hence cybersecurity); (3) and a paranoid one: complete security, if achievable, is not a permanent state (hence cyber(in)security). Cyberspace is conceived as a set of digital techniques used to exchange information but also as a new type of social space, partially virtual, which may constitute a being entirely separated from a physical one. A pivotal date for arising of cyberspace may be considered the year 1968 in which routing in the ARPANET network appeared and so did the first programmable logical controller (PLC). For cyberspace this will be the year 1976 – publishing of the key agreement protocol by Witfield Diffie and Martin Hellman. Development of security is correlated with warfare and armament – the military sector has historically made the most significant investments in this area.**

***Keywords*—cybersecurity, cryptology, conversation**

"*For millions of years, mankind lived just like the animals. Then something happened which unleashed the power of our imagination. We learned to talk and we learned to listen. Speech has allowed the communication of ideas, enabling human beings to work together to build the impossible. Mankind's greatest achievements have come about by talking, and its greatest failures by not talking. It doesn't have to be like this. Our greatest hopes could become reality in the future. With the technology at our disposal, the possibilities are unbounded. All we need to do is make sure we keep talking.*"
Prof. Stephen Hawking (1942-2018)

I. Introduction

In the course of evolution, humankind has developed its cognitive and adaptive abilities, in the pursuit of expansion in the ecosystem on Earth. Well-developed verbal communication has become one of the key skills of homo sapiens and finally led to a skill of conversation and conveying ideas and emotions through it. A conversation is an act in which the communicating parties talk and listen, and sometimes change their ideas and also emotions as a result of it. For thousands of years people have tried in various ways to understand the world around them, by developing various theories about relationships between - mainly physical – phenomena. Empedocles of Akragas established four elements: earth, water, air and fire. In Japanese culture void appears which also signifies heaven, in Chinese culture air disappears, and wood and metal appear. In Hinduism sound is distinguished as element. Theories of elements have their reference to nature which to a large extent was explored by humans through observation, less frequently through experiments. Elements have a physical, tangible character, they are to a significant degree deprived of control, though it is unquestionable that humans have a need to harness them.

The purpose of this paper is to present three theses:

1) a cultural one: cyberspace is an advanced technical and cultural creation – it is an embodiment of dreams of numerous creators, inventors and engineers,
2) a technical one: security and cyberspace are inseparable components (hence cybersecurity),
3) and a paranoid one: complete security, if achievable, is not a permanent state (hence cyber(in)security in the paper title).

The purpose of this paper is rather to inform than review, and the article consists of five chapters, the first one being this short introduction. The second chapter refers to genesis of cyberspace and security of the latter. The third one describes a course of conversation in cyberspace and related threats. The fourth one concerns variability and risk influencing dangerous liaisons which become crucial at designing security systems. The last chapter is a brief summary of this work.

II. Genesis of Cyberspace and Its Security

Cyberspace emerges in the history of humankind in the second half of 20th century. It is an outcome of a process of creating inventions and various theories, of which a large number facilitated communication. According to [1] cyberspace is on one hand a set of digital techniques to exchange information, but on the other, a new type of social space, partially virtual, which may constitute a being entirely separated from a physical one. Third, it is an environment in which contemporary communication occurs via a telecommunications network. In evolution psychology, a new term has been coined: homo cyberus [2] associated with cybersocialization. The term "CYBERSPACE" [3] (capitalized) appears in a

This scientific research work was co-financed by the European Union, project name: "The system for identification and monitoring of anomalies and risks in ICT networks." The amount financed by the European Union was EUR 1,044,534.63. The investment outlay value for the entire project was EUR 1,407,526.46. The subsidy was allocated from the European Regional Development Fund, Operational Programme "Smart Growth," sub-measure 1.1.1 "Industrial research and development work implemented by enterprises.".

Author is with 1. Faculty of Electronics and Information Technologies, Institute of Telecommunications, Cybersecurity Division, Warsaw University of Technology; 2. Cybersecurity and Data Science Research Centre; Warsaw University of Technology; 3. Cryptomage S.A.; Poland (e-mail: k.szczypiorski@tele.pw.edu.pl).

series of collages created in the years 1968-1970 by a Danish artist Susanne Ussing in cooperation with a Danish architect Karsten Hoff. A decade later, this term appears in literature – it is used by the creator of cyberpunk William Gibson [4]. While Ussing's collages are expressive visions of people fused into cybernetic forms, which may be perceived neutral, cyberpunk as a variety of science fiction focuses mainly on dark sides of digitalization of the world and contact of homo sapiens with machines. Thus, step by step, a new element emerges, deprived of physical features, in which laws of physics, such as Newton's laws of motion, including the law of universal gravitation, are no longer valid.

Security actually goes hand in hand with cyberspace from the very beginning, as its immanent part. First, understood rather naively at a physical level, as separation of crucial signals (for instance confidential ones) from the other, literally at the level of ducts and wiring (so called air gap). This obviously seems insufficient already at a first glimpse, therefore cryptology, and above all cryptography, become involved in protection of communication. Therefore, from the technical perspective an attempt may be made to correlate the emergence of cyberspace and occurrence of cyber(in)security in it with the development of modern cryptology (Figure 1). In turn, the development of cryptology itself and as a consequence – of cybersecurity – is closely related to warfare. Cryptology is a science in which two forces coexist: a synthesizing, constructive one (cryptography) and an analyzing, almost destructive one (cryptanalysis). Throughout history, these two forces have been driving one another, while competing against one another as well – cryptographic methods must be resistant to known cryptanalytical attacks. A sort of arms race commences, in which algorithms are improved, and a main indicator of their strength is the time of their protection, arising to a large extent from the key length. Currently, from the perspective of cryptanalysis, the end of this arms race is a vision of a quantum computer [5], and from the angle of cryptography – postquantum algorithms [6].

The end of World War I saw the turning point in the era of manual ciphers. Over a century ago, in 1917, the Vernam cipher was developed – a perfect cipher, the essence of which is performing modulo 2 addition of a message with a random key of the same length as the message (hence the name: one-time pad). Development of the first version of an electromechanical encryption machine Enigma [7] in Germany symbolizes entering the era of machine ciphers, which lasted until mid-Cold War. Marian Rejewski, Jerzy Różycki and Henryk Zygalski led to breaking Enigma, which resulted in its modernization (addition of further rotors) shortly before the outbreak of World War II. During the war, the improved Enigma was broken with the use of Bombe [8] – an electromechanical machine developed in Great Britain by Alan Turing based on the design and prototype of Rejewski's group, the so-called cryptologic bomb. In 1947, the first point-contact transistor was constructed by John Bardeen and Walter Houser Brattain. It became a starting point for the development of contemporary computing machines, which occurred within a decade. At the end of the machine cipher era, in 1968, routing was applied in ARPANET [9], and a Programmable Logic Controller – PLC [10] was developed. The year 1968 may be considered the date of cyberspace initiation. Internet in its original form emerges some seven years later [11].

The era of modern ciphers commences a year later following the occurrence of the Internet - in 1976 Witfield Diffie and Martin Hellman [12] published the first shared key exchange algorithm based on asymmetric algorithms, using the complexity of calculating discrete logarithms. Thus, 1976 can be considered a symbolic date of initiation of cybersecurity. A year later, the DES (Data Encryption Standard) symmetric block algorithm was accepted as a federal standard in the USA [13] and in 1981 became a private sector standard for the next two decades. In 1978, Ron Rivest, Adi Shamir and Leonard Adleman published a paper [14] concerning the first cryptosystem using the public key and the problem of the complexity of factoring large numbers, named RSA after the initials of their surnames.

Warfare remains the driving force behind cybersecurity today. In the USA, after the period of the Cold War, during which the Silicon Valley flourished [15], mainly through huge capital investments, the attacks of 11 September 2001 opened the stage of combat against generally understood terrorism. In turn, another world's leading country in cybersecurity - Israel, which after the end of World War II engaged in a long-lasting conflict with Palestine, adopted a similar model as the USA during the Cold War, namely investments in the arms industry, which has formally been closely linked to cyberspace for a decade. For example, in the USA the Cyber Command [16] was created in 2009 and it complements the actions of the US military forces so far linked to traditional elements (US Air Force - air, US Army - land, US Navy - water) in cyberspace.

Cyberspace is also present in industry. Looking at the classification introduced several years ago [17]:

- Industry 1.0: age of steam,
- Industry 2.0: age of electricity,
- Industry 3.0: age of computers,
- Industry 4.0: age of human-machine barrier disappearance, cyberspace appears in the so-called age of computers, where mass production is supported by machines.

Historically, mass production arose by adding electricity to industry, and industry itself - by supporting manual production with steam engines. The age of computers and controlling them using SCADA (Supervisory Control and Data Acquisition) systems would not have been possible without the aforementioned development of the Programmable Logic Controller (PLC) in 1968 [10]. Dick Morley, an American engineer and inventor, is considered the father of this invention. This device allowed the physical control of the machine and the execution of a specific algorithm necessary for the production process. On the other hand, industry 4.0 is largely based on attaching SCADA systems to the Internet (which has technically not been a problem for a long time) and on using solutions from the area of the Industrial Internet of Things [18]. In this case, a huge number of data requiring protection appears.

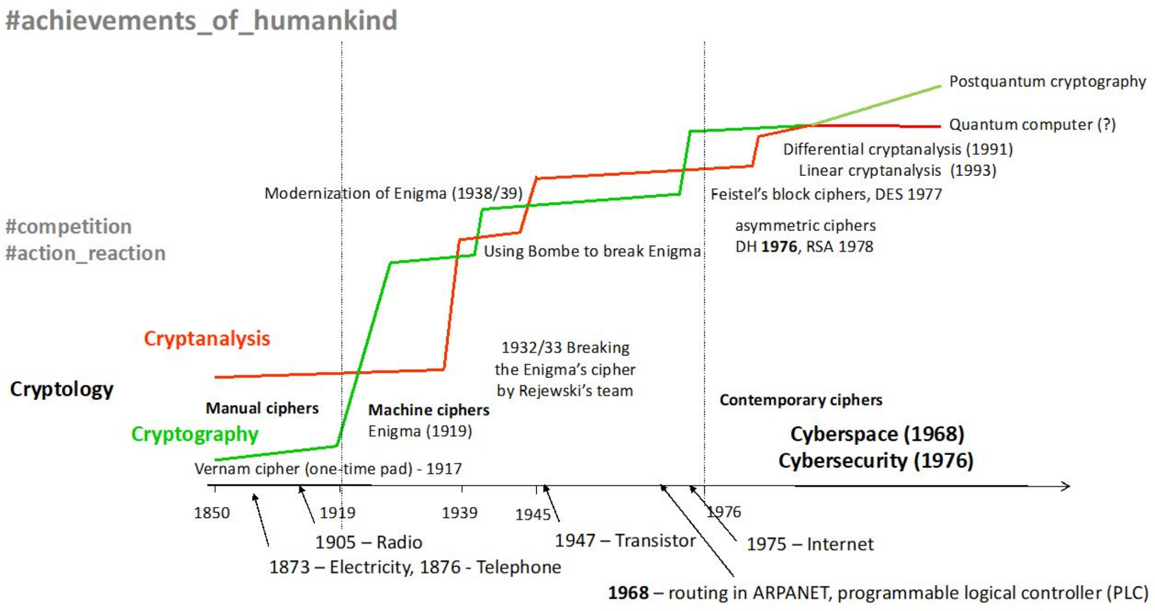

#achievements_of_humankind
#competition
#action_reaction
Cryptanalysis
Cryptology
Cryptography
Manual ciphers
Machine ciphers
Enigma (1919)
Vernam cipher (one-time pad) - 1917
Modernization of Enigma (1938/39)
Using Bombe to break Enigma
1932/33 Breaking the Enigma's cipher by Rejewski's team
Postquantum cryptography
Quantum computer (?)
Differential cryptanalysis (1991)
Linear cryptanalysis (1993)
Feistel's block ciphers, DES 1977
asymmetric ciphers
DH 1976, RSA 1978
Contemporary ciphers
Cyberspace (1968)
Cybersecurity (1976)
1850
1919
1939
1945
1976
1905 – Radio
1873 – Electricity, 1876 - Telephone
1947 – Transistor
1975 – Internet
1968 – routing in ARPANET, programmable logical controller (PLC)

Fig. 1. Cyberspace: origins against the background of modern cryptology

In summary, 1968 can be deemed to be the date of the emergence of cyberspace, both in the cultural and technical sense. Cybersecurity emerges 8 years later with the first algorithms using asymmetric cryptography.

III. Conversation in Cyberspace and Related Threats

Let us return to the topic of conversation (Figure 2(a)). Before speech enters cyberspace, it must be digitized, that is changed from an analogue to a digital form (Figure 2(b)). Digitization of the speech signal consists of two processes: sampling and quantization. According to Nyquist's sampling theorem, the sampling rate is twice the sampled channel and for example: 8 kHz for classical fixed-line telephony, 16 kHz or 22.050 kHz for medium quality (UKF radio) and 44.1 kHz or 48 kHz for compact disc quality (HiFi). Quantization is the process by which the samples are converted into fixed numerical values. This is how the data - which in this case are a conversion of speech to binary form - are generated.

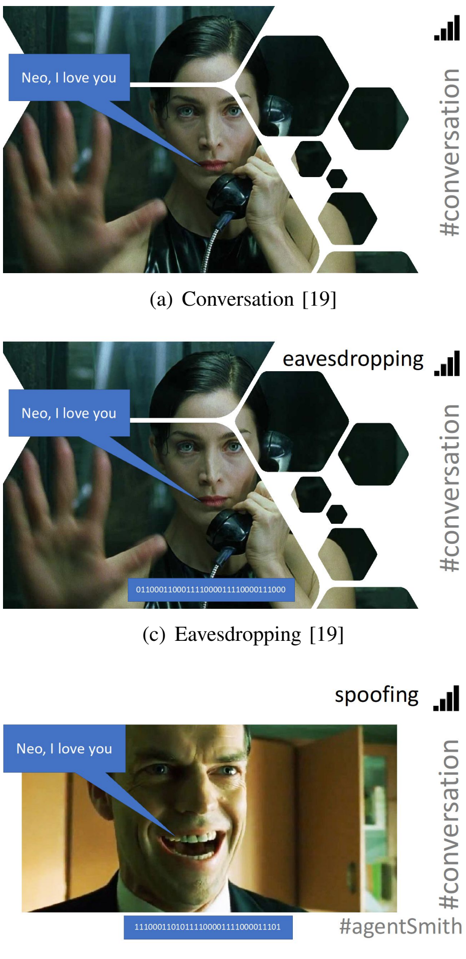
Data begin their journey in cyberspace: they can be transmitted (they are data "in motion"), stored or processed. At any time in the course of their journey, they may be eavesdropped (Figure 2(c)) or modified (Figure 2(d)). It is possible to spoof (Figure 2(e)) the sender (also the recipient) and to deny the fact of sending or receiving data (Figure 2(f)). These are the main threats to the data. Eavesdropping is a passive activity - it does not affect the structure of data, while the other three threats require taking action and, depending on the source of data, more or less engagement. It is easiest to operate on data created from the beginning to the end in cyberspace, and not, as in the example of a conversation, biometric data - then for instance modification is much easier to perform.

Data as such, without any context, are only a binary set; they are unstructured letters. They only gain value if they are information [21] that can already be compared to words. We can talk about both data protection and information protection. Nowadays, in times of availability of huge network bandwidth and computing power, there is a temptation to protect all data in an almost mindless way. It is desirable and reasonable to separate important information and to adapt appropriate protection methods to it. This is due to the fact that the "lifespan" of particular information, and thus a potential need to protect it is different, e.g. the location of General Dynamics F-16 Fighting Falcon multi-purpose planes over Poland is at the level of several dozen minutes, and the identity of spies is at least half a century.

On the basis of information we are able to build knowledge, which in the context of cyberspace is storing relevant information, searching for relationships and drawing conclusions. We can compare knowledge to sentences or even thoughts. At the end of the data processing chain we can place wisdom as the ability to make the right (whatever that means!) decisions based on the acquired knowledge.

In the context of the above mentioned threats (eavesdropping, modification, spoofing, denial), basic cybersecurity services are introduced [22]: confidentiality, integrity, authentication and non-repudiation. This set is complemented by an access control service which allows to control the rights to use resources.

Information protection services are built with different mechanisms: one of them is encryption lying in the area of cryptography. As I mentioned in the previous chapter, the main measure of the strength of cryptographic algorithms is the time of their protection, resulting to a large extent from the key length. With the classical model of computation techniques development, it is possible to predict the chance of breaking the protected information (also based on Moore's law) and thus



(a) Conversation [19]

(b) Speech digitization – data occur [19]

(c) Eavesdropping [19]

(d) Modification [19]

(e) Spoofing [20]

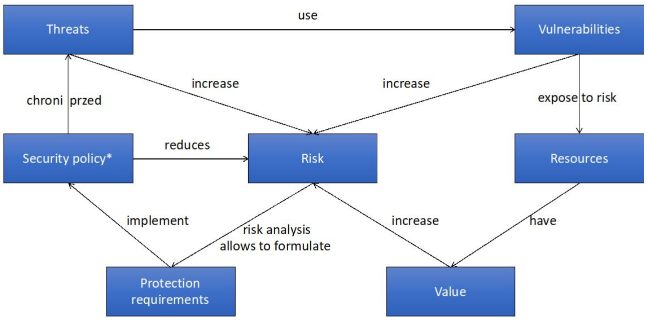
(f) Denial [19]

Fig. 2. Security attacks

offer protection for an agreed period. Two major issues arise: the first one is the skillful management of keys, which includes their generation, distribution, storage, and destruction after use. The second one is the algorithm's resistance to known cryptanalytic attacks, as well as a design that is resistant to so-called backdoor, that is ways of faster conversion of certain properties using the weak features of the algorithm [23].

IV. Dangerous Liaisons: Designing Security Systems

Threats are the root cause of taking measures in cybersecurity area. Threats (Figure 3) exploit vulnerabilities that arise during the design, implementation or configuration of ICT systems. Vulnerabilities (like threats) increase the risk, which is an indicator of a condition or event that can lead to losses. Vulnerabilities expose to risk resources that are of value (not only economic). The greater the value, the potentially greater the risk. The security policy defines security measures at the organizational and technical level and thus reduces risk and protects against threats. On the other hand, the security requirements implement the security policy and thanks to the risk analysis [24], which is crucial in designing security measures, it is possible to formulate them. It is worth noting that the security policy introduces new resources along with new vulnerabilities specific to them.



*Security policy specifies security measures which also become resources (with vulnerabilities)

Fig. 3. Dangerous liaisons

The risk analysis, which consists in predicting the negative effects of actions and phenomena and relevant reduction of potential losses arising from such situations, is a process (Figure 4) which, as mentioned earlier, results in a draft security policy. Such a project is subject to cost estimation. It is an iterative process – adoption of an acceptable level of risk at acceptable costs provides a starting point for the adoption of the security policy, and at the same time it is continuous – during the operation of security systems it should be carried out periodically.

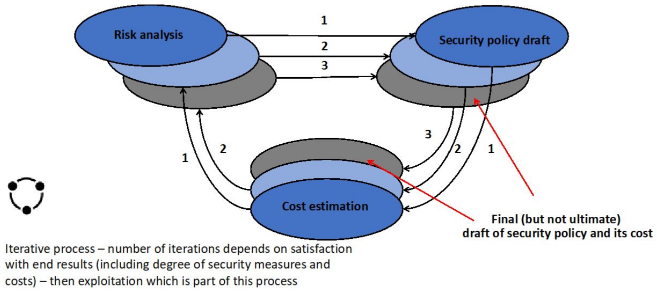

Risk analysis
Security policy draft
Cost estimation
1
2
3
1
2
3
2
1
Final (but not ultimate)
draft of security policy and its cost
Iterative process – number of iterations depends on satisfaction with end results (including degree of security measures and costs) – then exploitation which is part of this process

Fig. 4. Designing security systems

An ICT system can be observed through its components and relations between them [25]. In each object we can observe features that may be permanent, but some of them may change. Change is related to the transition of a feature to another one. The observation of a feature is only important if something can be done about the information about the change of the feature. Not every observation is therefore valuable from a practical point of view. Many features may be distinguished for observation in an object, but in many cases we do not have full knowledge of all features. At the same time, some features may appear unexpectedly and others may disappear. On the other hand, some of the features are not significant for the observation of the change or, what is worse, the observer is not aware of their significance. After distinguishing a particular feature, a change in the property of the feature is observed compared to various measures, often calculated on the basis of previous observation periods. In the case of ICT networks, the object is usually the telecommunications protocol. For each protocol, a separate model is built, distinguishing important features such as connectivity, retransmission mechanisms, support of delayed or damaged data units. In the examination of each of these aspects, the network parameters associated with a given feature in retransmission mechanisms (timeout counters, retransmission window size, error rate) are analyzed. Identifying a difference in the protocol profile is a sign of change and is very likely to mean a network attack. Building knowledge on the basis of information, which is an unambiguous indication for an attack, facilitates the creation of appropriate signatures, while phenomena that are unrecognized to some extent have the status of anomalies. In the operation of security systems, the issue of false alarms affects the reliability of systems detecting anomalies, in particular false positives lead to the non-recognition of attacks. False negatives consume resources, but are not critical for systems security (something that is not an attack in reality, is treated as an attack).

V. Summary

Cyberspace is an advanced product of human imagination not only in the technical sense, but also in the socio-cultural one. Thanks to technology, the vision created entirely in the human mind has become reality - it is an example of a dream come true.

Cyberspace permeates the physical world, although it can be completely virtual. By its nature it is inseparable from security, which is variable. and is never complete, thus the "cyber(in)security" in the title.

People (including the author of the initial quote) have long dreamt of space exploration, and perhaps also of transferring life to an alien planet. Meanwhile, we have cyberspace, and perhaps we will be able to replicate ourselves in it and thanks to this we will become immortal and fully happy. This motif is known from science fiction (e.g. from the film "Lucy" directed and screenplay by Luc Besson [26]) and perhaps needs to be revised.

References

[1] Wikipedia contributors, "Cyberspace — Wikipedia, The Free Encyclopedia," https://en.wikipedia.org/wiki/Cyberspace, 2020, [Online; accessed 3-February-2020].

[2] V. Pleszakov, https://www.litres.ru/vladimir-pleshakov/kibersocializaciya-cheloveka-ot-homo-sapiens-a-do-homo-cyberus-a/, 2012.

[3] J. Lillemose and M. Kryger, "The (Re)invention of Cyberspace – Kunstkritikk," https://kunstkritikk.com/the-reinvention-of-cyberspace/, 2015, [Online; accessed 3-February-2020].

[4] Wikipedia contributors, "William Gibson — Wikipedia, The Free Encyclopedia," https://en.wikipedia.org/w/index.php?title=William_Gibson&oldid=937885621, 2020, [Online; accessed 3-February-2020].

[5] F. Arute, K. Arya, R. Babbush, D. Bacon, J. Bardin, R. Barends, R. Biswas, S. Boixo, F. Brandao, D. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, and J. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, 10 2019.

[6] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017. [Online]. Available: http://dx.doi.org/10.1038/nature23461

[7] Wikipedia contributors, "Enigma machine — Wikipedia, The Free Encyclopedia," https://en.wikipedia.org/wiki/Enigma_machine, 2020, [Online; accessed 3-February-2020].

[8] Crypto Museum, "Bombe," https://www.cryptomuseum.com/crypto/bombe/, 2020, [Online; accessed 3-February-2020].

[9] B. Leiner, V. Cerf, D. Clark, R. Kahn, L. Kleinrock, D. Lynch, J. Postel, L. Roberts, and S. Wolff, "A brief history of the internet," *Computer Communication Review*, vol. 39, pp. 22–31, 10 2009.

[10] AutomationDirect.com, "History of the PLC," https://library.automationdirect.com/history-of-the-plc/, 2020, [Online; accessed 3-February-2020].

[11] "Specification of Internet Transmission Control Program," RFC 675, Dec. 1974. [Online]. Available: https://rfc-editor.org/rfc/rfc675.txt

[12] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theor.*, vol. 22, no. 6, p. 644–654, Sep. 2006. [Online]. Available: https://doi.org/10.1109/TIT.1976.1055638

[13] Des, "Data encryption standard," in *In FIPS PUB 46, Federal Information Processing Standards Publication*, 1977, pp. 46–2.

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, p. 120–126, Feb. 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[15] Wikipedia contributors, "Silicon valley — Wikipedia, the free encyclopedia," https://en.wikipedia.org/wiki/Silicon_Valley, 2020, [Online; accessed 3-February-2020].

[16] U.S. Army Cyber Command, "Army Cyber Command Home," https://www.arcyber.army.mil/, 2020, [Online; accessed 3-February-2020].

[17] BMBF-Internetredaktion, "Industrie 4.0 - BMBF," https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html, 2020, [Online; accessed 3-February-2020].

[18] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," *Computers in Industry*, vol. 101, pp. 1–12, 10 2018.

[19] [accessed 3-February-2020]. [Online]. Available: https://glavcom.ua/scotch/showbiz/kultovaya-trilogiya-matrica-oficialno-poluchit-perezapusk-483980/g358176.html

[20] “The Matrix Fan Theory Puts Agent Smith As The One, And It Kind Of Works - CINEMABLEND,” https://www.cinemablend.com/new/Matrix-Fan-Theory-Puts-Agent-Smith-One-It-Kind-Works-121077.html, 2020, [Online; accessed 3-February-2020].

[21] B. Stafanowicz, “Informacja, wiedza, madrość,” *Biblioteka Wiadomości Statystycznych, t.66*, 2013.

[22] ISO, “7498-2. information processing systems open systems interconnection basic reference model-part 2: Security architecture,” *ISO Geneva, Switzerland*, 1989.

[23] N. Perlroth, J. Larson, and S. Shane, “N.S.A. Able to Foil Basic Safeguards of Privacy on Web,” https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html, 2013, [Online; accessed 3-February-2020].

[24] ISO, “Risk Management-Guidelines (Standard No. ISO 31000: 2018),” *ISO*, vol. 31000, 2018.

[25] J. Bieniasz, M. Stepkowska, A. Janicki, and K. Szczypiorski, “Mobile agents for detecting network attacks using timing covert channels,” *J. UCS*, vol. 25, no. 9, pp. 1109–1130, 2019. [Online]. Available: http://www.jucs.org/jucs_25_9/mobile_agents_for_detecting

[26] “Lucy (2014),” https://www.imdb.com/title/tt2872732/, 2014, [Online; accessed 3-February-2020].