JOURNAL OF MODERN SCIENCE

TOM 4/53/2023

www.jomswsge.com

DOI: doi.org/10.13166/jms/175514

ARNOLD WARCHAŁ
Military University of Technology, Poland
ORCID iD: 0000-0001-6495-643X

KAZIMIERZ PIOTRKOWSKI
Military University of Technology, Poland
ORCID iD: 0000-0003-2001-1826

INFORMATION AND MODERN TECHNOLOGIES AS AN ASYMMETRIC THREAT TO STATE SECURITY. PHILOSOPHICAL PERSPECTIVE.

Abstract

Rapid evolution and progress in computer sciences present new determinants for informational technologies. The universal knowledge based on Mathematics and Computer science exploring processes in information dissemination, should be persistently analyzed. Its focus on practical applicability presents various problems and new possibilities for the field of Security Studies, adding new categories to its research interests, that should be constantly defined and redefined. And what is the objective of the article. The predicaments of technological evolution in view o the categories arising through philosophical focus, presented here by authors and as applied in Security studies, point to definitions and associated categories of potential dangers that IT progress may entail. Hence, the presentation of three categories analyzed – information, communication, asymmetric threat, and the following analysis of categories of threats with asymmetric values, as a potential nuisance and danger to state security, related to those categories. The descriptive methodology used in the article is limited to a presentation of philosophical categories, as it allows for defining of chosen problems that correspond, upon analysis, to asymmetric threats mounting from IT evolution. And as is concluded, the new developments, as discussed in the article, present challenges for state security and are presently evolving. Hence, those should be constantly categorized and associated with security predicaments – active and potential.

Keywords: *asymmetric threats, communication, information, IT, Security studies*

Remarks on information, communication, and asymmetric threats as philosophical categories

It's only a truism, that our contemporary world evolves around information. We live in an information society, and overall, we live in a global information civilization. Regardless of civilizational-cultural differences, information as the general mode of life experience and societal interaction is of preeminent importance on all levels of sociopolitical and institutional life for all developed and developing countries. Its constructive characteristics, nonetheless, may be shadowed by the negative effects of a threat cast on society unprepared for its various predicaments of technological progress. Whatever the nature of information is, and whatever the technics and technologies employed to communicate its determinants or solutions are effective, information can have a dual nature – from the ethical perspective and have ontologically creative and destructive potential at the outset of discussion on its nature. There is already a field in Philosophy dedicated to information – Philosophy of Information, that *[…] may be defined as the philosophical field concerned with (a) the critical investigation of the conceptual nature and basic principles of information, including its dynamics, utilization, and sciences, and (b) the elaboration and application of information-theoretic and computational methodologies to philosophical problems* (Floridi, 2009, pp. 153 – 158). This field of philosophy is a perspective on various dimensions of phenomena of information, however, philosophical discussion is not always generative of its subject. It is due mainly to new technologies, usually engineered for particular goals, not necessarily created for understanding of imminent nature of information itself, or in unison with the philosophical perspectives bordering, when approaching a question mark, on metaphysical speculations or old epistemological theories.

Philosophical perspectives are verbal in their discourse and usually concentrate on information as the outcome of human cognition, with its capacity to accept, form and create types of knowledge, and informational cycle. The studies in the field, abstracting of old epistemological values, were done in XIX c. by Charles S. Pierce, with his theory of semiotics. Other propositions were developed in XX c. by Martin Heidegger, Hans-Georg Gadamer, Jean-François Lyotard, and Gilbert Simondon, to name a few. However, at the turn of the XXI c., it was Luciano Floridi, an Italian philosopher, who has extensively written on the philosophy of information, and who coined the name *philosophy of information*. He has developed the influential theory of the Philosophy of Information (PI) and the concept of the *infosphere*, by exploring the ethical, epistemological, and ontological dimensions of information and its impact on our understanding of reality, knowledge, and communication. The philosophical theories of information usually border those of communication and explore various aspects of information and communication affecting society and justification of its processes. It is worth noting that the older theories on information are encompassed by a wider sphere of analysis of other philosophical focus, as is stated that: *Until the second half of the twentieth century* *almost no modern philosopher considered "information* to be an important philosophical concept. The term has no lemma in the well-known encyclopedia of Edwards (1967) and is not mentioned in Windelband (1903). In this context the interest in *Philosophy of Information* is a recent development." (Adriaans, 2020, SEofPh.)

There are other academic endeavors concerning information as a social construct or cultural mechanisms that would steer us toward the philosophy of mathematics responsible for various advancements in theoretical and applied sciences, including Physics, Mathematics, or Cybernetics, and in Computer Sciences, with mathematical theories as explanations for the formation of variables and logical conclusions. Information theory is considered to be the founding pattern for the others. It is co-joined with applied and applicable mathematics, and computer science, and, as is widely recognized, was founded by American mathematician and electrical engineer Claude Shannon. His seminal work, *A Mathematical Theory of Communication,* (Shannon,1948) laid the foundation for information theory and revolutionized the field of communication and data transmission. In his work, he introduced fundamental concepts and principles that form the basis of information theory. He quantified information, introduced the notion of entropy as a measure of information uncertainty, and established the concept of channel capacity for optimal data transmission. Shannon's groundbreaking contributions provided a mathematical framework for analyzing the fundamental limits and efficiency of communication systems (Stone, J V., 2018/02/16,). Claude Shannon's work continues to be highly influential in various domains, including telecommunications, computer science, cryptography, data compression, and statistical inference. His information theory has paved the way for advancements in digital communication, data storage, and information processing, playing a crucial role in shaping modern technologies. There have been, of course, subsequent contributions and developments in information theory by numerous researchers and scholars, building upon Shannon's foundational work.

Many authors writing on information as a philosophical category would consider its synonym – communication. While those are interconnected, they represent different aspects of the exchange and transmission of knowledge or messages. The meaning of information and the meaning of communication are different. Information refers to processed or organized data that carries meaning or significance. It represents knowledge or facts that are communicated or received. Information can exist independently of communication, stored in various forms, such as books, databases, or digital files. It can be transmitted or shared through communication channels. Communication, on the other hand, is the process of transmitting or exchanging information between individuals or entities. It involves the encoding, transmission, and decoding of messages between a sender and a receiver. Communication encompasses not only the transmission of information but also the social interaction, interpretation, and understanding of messages. In other words, communication is a means through which information is conveyed, shared, or exchanged between individuals, groups, or systems. It involves the use of language, symbols, gestures, or other mediums to convey information from a sender to a receiver. They are interdependent, however, as effective communication relies on the accurate and meaningful exchange of information, while information requires communication channels to be shared or transmitted;

The topic of asymmetric threats is, of course as old as the historical description of warfare, politics, strategies, and tactics, nonetheless, new as a category of security studies (for the comprehensive and referential discussion on the topic see: Stojanovic, S, 2018). Within the systemic political activity of teleological importance, its essence lies in the unequal distribution of potential means of activity using measures differently than the typical for a given political action, including warfare, undermining at first the state's ability to counteract threats and attacks of various means. The effectiveness of asymmetry can be determined by the potentiality of achieving or surpassing the strategic importance, with the tactical and singular ability of a lesser/weaker agent undermining the position of a stronger one. Technological progress generates this ability, not just for political entities but also for individuals of a terrorist set of mind. This ability is based either on a slow-paced prolonged process aimed at the socio-political or military institution or the ability to use technological progress to a particular advantage. One of the easiest ways to act within asymmetrical settings is through informational technology, by adapting advanced computing, using AI, intrusion in computer systems, and process of information dissemination. However, in security studies, apart from strategic and military outlook (Benett, B W., 2003, pp. 33 – 66), no theoretical interpretative model is definitive for asymmetric threat, since the categories of asymmetric threats are still defined. Hence, the focus on the preliminary process of an eidetic proportion needs to be clarified. The various categories of asymmetric threats are already known (Ćurčić, 2018). However, the evolution of information technology presents an ever-changing environment for security. Information technology is susceptible to being used belligerently. Those, with knowledge can use it against a stronger opponent.

Considering the topic of this short, philosophical discussion, its aim is portrayal of fundamental changes determinative of general security predicaments, and as analyzing threat categories corresponding to contemporary technological advancements, that changes the infosphere of various human activities, and potentially the entire socio-political system of a given domain. Chosen categories of asymmetric danger are compared in the article, categorized in the manner presenting perspectives of various authors from different disciplines. The article is mainly descriptive in its character. It methodologically stops at naming categories, found in discussion on contemporary phenomenon of IT, and short of the eidetic reduction aims to define those that coincide or overlap with a categories of asymmetric threats.

Information, and communication as the asymmetric threats.

Today information and communication are the basis for information society livelihoods. Undermining the core values of meaning can be lethal to its harmony, and, given the means of tools available to change meaning in the society that dwells on information, anyone capable of using those tools can become a political entity in a negative sense. Information civilization is, therefore, susceptible to lies, on one side, and corruptible practical ability based on technical knowledge to control various means of communication by individuals, on the other, affects the individual and general security in the internet, or through the internet and other means of digital transfers. What makes information (and communication) special in Security studies, is that such categories can be considered as universal for any form of conscious interaction with reality, determining the final value of importance, by those with means and merits. It is especially important to understand, if we realize that technology, where information and communication are of essence, is critical to national and international security, since anyone with knowledge, and not necessarily institutional, can become a *weapon* operator, making information an asymmetric threat, using propaganda or digitally endangering critical infrastructure (see Stavroulakis, Stamp, 2010). Therefore, the field of Security studies and its now important topics corresponds directly to the endeavors of Computer science.

When we consider *computer sciences* there are phenomena that determine others alive. In that applied scientific field extent of changes can be observed based on solutions to particular informational problems – of how to change the intangibles into observable phenomena controlling the mechanism of biological life. We can abstract processes of this Pythagorean in nature, harmony – mathematically underlying metaphysical interest of ontological *reality.* It has to do with the exchange of given *universals* (believed to exist as a unity of values extracted into particular experiences of individual life. Its particularity rests in a social understanding that mathematical knowledge equals the logic of symmetry of values, symmetrical in an alchemical sense of combining the theoretical mind with an empirical essence of objective experience. If there was a search for the alchemical fountain of youth, the fountain of youth became a mathematical reality in computer sciences. Anyone who observed the process of its evolution, as the authors here did, understands given simple programming languages – like Fortran, Lisp, COBOL, or Basic (see internet CHM – Computer History Museum) nuances of mathematical equations and semiotic values coming alive on a computer screen.

There is the unifying value of numbers that is natural, that there is logical synchronization within the world, as was discovered with the Pythagorean harmony of numbers (Russell, 1945, pp 29-37), or Galilean agreement that mathematics is the fundament of understanding nature (Jespph, D, 2016, pp. 160 – 177), or Eulerian understanding that numbers are proportions of measure leading to a unifying value of numbers that is natural reality (see Euler, Leonard, Elements of Algebra, pp. 1 – 2, ed. 1822). We are happy to live in times of computer transmutation of algorithms into creative transmutation of our human idea, or determinants of who we are, looking into the mirror of our consciousness and becoming ontological, measurable identity with the thought, individual thought process extending and leading back to mathematical/metaphysical reality. Its semiotic value depends on logical creativity and meaning that we expose from our consciousness, which is very individual in its effects. How it interacts with the *material* can be adjusted with knowledge and technological solution, where universal knowledge is used by anyone and for whatever purpose. This interactivity evolved into what is known today as VR – virtual reality and AR – augmented reality (XR in general), with the looming another side of mathematics and information, AI – Artificial Intelligence, that became a potential threat, besides the previous fears.

New fears evolved because of information transcoding reality. Information can be considered an asymmetric threat in certain contexts of cybersecurity (Nir Kshetri, Information and Communications Technologies, Cyberattacks, and Strategic Asymmetry, 2010, pp 119 – 137). The threat is asymmetric when there is an imbalance in access, control, or understanding of information between parties. Exploiting this imbalance can provide advantages to asymmetric actors, allowing them to manipulate, deceive, disrupt, or gain upper hand in a conflict or power dynamic due to the following reasons for asymmetry: Information Imbalance, Strategic Deception, Cyber Warfare, Non-traditional Threats, and Insider Threats.

In asymmetric conflicts or power dynamics, one party may possess superior or privileged information compared to the other (Kimberly Navala, Addressing Information Imbalances, 2022). This information imbalance can give the more informed party a significant advantage, allowing them to manipulate perceptions, influence decisions, or exploit vulnerabilities in the less informed party. Information imbalances are easily generated using IT; Information warfare, propaganda, or disinformation campaigns are examples of how asymmetric actors may exploit information for their benefit. Deliberate misinformation or deception tactics (Reid et. al., 2017, pp 81 – 101), can be used as an asymmetric strategy. By spreading false or misleading information, an entity can confuse, misdirect, or misinform its adversaries, creating a strategic advantage. This is the level of strategic deception organized at the level of strategic planning; The next category is that of Cyber Warfare. In the digital realm, information can be weaponized by malicious actors. Cyberattacks, such as hacking, data breaches, or disruptive actions, can exploit vulnerabilities in information systems and networks (Haughey, Dec. 22, 2021). By gaining unauthorized access to sensitive information or disrupting critical infrastructure, asymmetric actors can cause significant harm and disruption, on the non-military and military levels; Non-traditional Threats: Information can be used as a tool for unconventional threats, such as terrorism or insurgency. Terrorist organizations, for instance, may utilize online platforms and social media to disseminate propaganda, recruit members, coordinate attacks, or spread fear. The asymmetric nature of such threats lies in their ability to leverage information to achieve their objectives with minimal resources and asymmetric tactics. (See Jumbis, 2011); The Insider threat is the last category of reasons for asymmetry. Information can become an asymmetric threat when it is compromised or misused by insiders with privileged access to sensitive data. Insider threats, whether through espionage, data theft, or sabotage, can lead to significant damage for organizations, governments, or individuals. The insider knowledge of the organizational operations and systems can make the threat hard to detect and counter (Dziwa, 21 Oct., 2021).

Combining information with communication as a part of the informational process poses additional issues. While Communication is not inherently asymmetric, it can be used as a tool or means to create an asymmetric threat under certain circumstances. Here are examples where communication becomes an asymmetric threat: Propaganda and Psychological Warfare: Asymmetric actors may use communication techniques, such as propaganda and psychological operations, to manipulate perceptions, sow discord, or influence public opinion. By disseminating false or misleading information, they can shape narratives, create divisions, or undermine trust in established institutions or governments; Media Manipulation: Controlling or manipulating media channels is an asymmetric tactic. Manipulation of information processes in media outlets can spread biased or distorted information, amplify their own narratives, and suppress opposing viewpoints (Carpenter, 2020). Significant impact on shaping public opinion and perceptions lead to asymmetries in information access and influence; Information Manipulation in Conflict: In asymmetric conflicts, communication can become a weapon to mislead, confuse, or deceive adversaries. Disinformation campaigns, fake news, or strategic leaks of false information employed to undermine decision-making, planning, or morale are other examples. This asymmetry can exploit vulnerabilities and create confusion or miscalculations in the adversary's perception and response; Cyber Communication Attacks: Asymmetric actors may employ cyber communication attacks as a form of the asymmetric threat. These attacks can involve hacking, defacement, and manipulation of websites, social media accounts, or communication channels. By disrupting or manipulating the flow of information, they can undermine trust, sow chaos, or disrupt critical operations; Communication Control: In several contexts, the control or restriction of communication can also become an asymmetric threat. For example, authoritarian regimes may employ censorship, surveillance, or internet shutdowns to stifle dissent, control information flow, and maintain their grip on power. In general, asymmetry in communication capabilities limits the ability of individuals or opposition groups to express themselves or organize effectively; The above categories are, of course, not exhaustive in discussions focused on information and IT, and asymmetric threats.

Conclusion

The knowledge of computer science, and the knowledge of security studies, are intertwined. The above-presented reasons for evolving categories generative of evolutionary process of information and communication are looked at primarily through methodological perspective of philosophy – categorial analysis and explanation. In this sense, both fields have similar academic capabilities: to generate their own system knowledge, to co-determine other research, and to construct unified applications for academic research, as in this case, focused on asymmetric threats arising from technological advancements. The discussion and findings focused on current advancements in IT are explanatory for the institutional changes in the security realm of State goals, of a military and non-military kind, as well as on other institutional or individual levels. It is crucial for states to develop robust cybersecurity measures, invest in technological capabilities, and enhance their ability to detect, prevent, and respond to asymmetric threats posed by information and new technologies in order to fulfill their obligations for protection against present and potential dangers. Regardless of this ability, venturing into a new territory of evolutionary knowledge brings alive new threats. However, those threats seldom evolve by themselves, often evolve because of human involvement, and creativity to use, the created to their own advantage.

It is the search for the advantage that brings asymmetric threats alive on many functional levels of state and individual activity. If we live in information society, then we are susceptible to information warfare. The increasing reliance on information and communication technologies has opened up new avenues for state and non-state actors to engage in information warfare. By leveraging cyber capabilities, such as hacking, disinformation campaigns, or propaganda dissemination, malicious actors can exploit vulnerabilities in information systems to undermine state security. These asymmetric tactics can disrupt critical infrastructure, compromise sensitive information, or manipulate public opinion. On the individual and institutional levels, new technologies and interconnected systems have increased the risk of cyber attacks, which can pose asymmetric threats to state security. Sophisticated adversaries can exploit vulnerabilities in government networks, critical infrastructure, or military systems, causing significant damage or disruption. Asymmetric actors with limited resources can leverage cyber tools to target states with superior technological capabilities.

Emerging technologies like artificial intelligence, drones, and autonomous systems can pose asymmetric threats when used by state or non-state actors in ways that challenge traditional security paradigms. Disruptive technologies, the use of drones for surveillance or weapon delivery can provide asymmetric advantages to non-state actors, allowing them to bypass conventional defenses and project power in ways that are difficult to counter (Drew, 2023). Emerging technologies allow for information influence and manipulation. The proliferation of social media and digital platforms has enabled the rapid dissemination of information and spread of disinformation or propaganda. State and non-state actors can use these channels to manipulate public opinion, sow discord, or exploit societal fault lines. The asymmetric nature of these threats lies in their ability to exert influence and destabilize states without the need for conventional military capabilities.

The internet used universally is an interconnected dimension with great information storage places. It is open to cyber espionage and intellectual property theft. State-sponsored or state-supported cyber espionage activities can result in the theft of sensitive government information, intellectual property, or trade secrets. Such asymmetric actions can provide an advantage to the perpetrator by acquiring valuable knowledge, undermining a state's competitiveness, or gaining insights into military strategies or diplomatic negotiations. And last but not least, it is great field of knowledge, and a field generative of knowledge. Asymmetric access to technology can also be a threat. The digital divide and disparities in technological capabilities between states can also create asymmetric threats. States with limited technological infrastructure or resources may face vulnerabilities in critical sectors such as cybersecurity, telecommunications, or digital governance (Van Dijk, 2019). Asymmetric actors can exploit these weaknesses, gaining access to state secrets or disrupting essential services. Knowledge is power, and information is its tool. It is a tool or a weapon, depends on who uses it. Threats are imminent, but so is the preventive activity of the state and financial capability to sensify the state security system to real and potential dangers. Addressing these asymmetric threats requires a combination of technological safeguards, user education, ethical guidelines, regulatory frameworks, and rather a vivid imagination looking at potential of the evolving informational asymmetry with the AI already in use.

References

Adriaans, P. (2020). *Information*, The Stanford Encyclopedia of Philosophy (Fall 2020 Edition), Edward N. Zalta (ed.); https://plato.stanford.edu/archives/fall2020/entries/information/

Bennett, B. W. (2003). et al. *Responding to asymmetric threats.* New Challenges, New Tools for Defense Decision-making, 1st ed., RAND Corporation, pp. 33–66. JSTOR, http://www.jstor.org/stable/10.7249/mr1576rc.11.

Carpenter, P. (2020). *The dangerous art of media and messaging manipulation*, Forbes, Int. ed., 2020/08/03, https://www.forbes.com/sites/forbesbusinesscouncil/2020/08/03/the-dangerous-art-of-social-media-and-messaging-manipulation/?sh=4b661cdf3f69

CHM – Computer History Museum, https://www.computerhistory.org/timeline/software-languages/

Ćurčić, M. (2018). Asymmetric Threats in Security Studies, In: Stojanovic, Stanislav, ed., Asymmetry and Strategy. Thematic Collection of Articles, Strategic Research Institute & National Defence School.

Belgrade, http://www.isi.mod.gov.rs/multimedia/dodaci/themati_collection_of_articles_asymmetry_and_strat_1550753449.pdf

Van Dijk, J. A.G.M. (2019). The Digital Divide, Polly Press, https://www.researchgate.net/publication/336775102_The_Digital_Divide

Drew, C. (2022). 22 Disruptive Technology Examples. Helpful Professor. https://helpfulprofessor.com/disruptive-technology-examples/

Dzambic, M. (2023). *NATO's New Strategic Concept: Non-Traditional Threats and Bridging Military Capability Gaps.* Connections, vol. 10, no. 3, 2011, pp. 14–36. JSTOR, http://www.jstor.org/stable/26326242. Accessed 30 May 2023

Dziwa, A. A. (2021). The Invisible Enemy Within: Insider Threats, 21 October 2021, https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-invisible-enemy-within-insider-threats

Euler, L. (1822). Elements of Algebra, ed. 1822,https://archive.org/details/in.ernet.dli.2015.513805/page/n3/mode/2up

Floridi, L. (2009). The Information Society and Its Philosophy: Introduction to the Special Issue on The Philosophy of Information, Its Nature, and Future Developments, May 2009, The Information Society 25(3):153-158; https://www.researchgate.net/publication/220175461_The_Information_Society_and_Its_Philosophy_Introduction_to_the_Special_Issue_on_The_Philosophy_of_Information_Its_Nature_and_Future_Developments

Haughey, C. J. (2021). Cyber Warfare: What To Expect in 2022 Dec. 22, 2021
https://securityintelligence.com/articles/cyber-warfare-what-to-expect-2022/

Jesseph, D. (2016). *Ratios, Quotients, And the Language of Nature.* The Language of Nature: Reassessing the Mathematization of Natural Philosophy in the Seventeenth Century, edited by Geoffrey Gorham et al., University of Minnesota Press, pp. 160–77. JSTOR, https://doi.org/10.5749/j.ctt1d390rg.9.

Johnson, S.E. (2003). et al. New Challenges, New Tools for Defense Decisionmaking. 1st ed., RAND Corporation, 2003. JSTOR, http://www.jstor.org/stable/10.7249/mr1576rc. Accessed 29 May 2023.

Kshetri, N. (2010). Information and Communications Technologies, Cyberattacks, and Strategic Asymmetry. In: The Global Cybercrime Industry. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-11522-6_6

Navala, K. (2022). Addressing Information Imbalances, Big Data Quarterly, Sept. 29, 2022, https://www.dbta.com/BigDataQuarterly/Articles/Addressing-Information-Imbalances-155172.aspx

Reid, I.D., Gozna, L.F., Boon, J.CW. (2017). *From Tactical to Strategic Deception Detection: Application of Psychological Synthesis.* Journal of Strategic Security 10, no. 1 (2017) : 81-101. Available at: https://digitalcommons.usf.edu/jss/vol10/iss1/6

Russell, B. (1945). History of Western Philosophy, Simon & Schuster, New York, https://ia803200.us.archive.org/10/items/TheHistoryOfWesternPhilosophy/HistoryOfWesternPhilosophy-BertrandRussell.pdf

Shannon, C.E. (1948). *A Mathematical Theory of Communication*, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948. https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

Stavroulakis, P., Stamp, M. (2010). Handbook of Information and Communication Security, https://www.researchgate.net/publication/242506688_Handbook_of_Information_and_Communication_Security

Stojanovic, S., ed. (2018). Asymmetry and Strategy. Thematic Collection of Articles, Strategic Research Institute & National Defence School, Belgrade, http://www.isi.mod.gov.rs/multimedia/dodaci/themati_collection_of_articles_asymmetry_and_strat_1550753449.pdf

Stone, J.V. (2018). Information Theory: A Tutorial Introduction, 2018/02/16, https://www.researchgate.net/publication/323257248_Information_Theory_A_Tutorial_Introduction