Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Piotr Dela, *Connections QJ* 15, no. 3 (2016): 55-64
https://doi.org/10.11610/Connections.15.3.05

Research Article

Cyberspace as the Environment Affected by Organized Crime Activity

Piotr Dela

War Studies University, Warsaw, Poland, http://www.akademia.mil.pl

Abstract: This article provides an overview of the main issues surrounding the use of cyberspace as the field on which information warfare is waged. It also investigates the role of organized criminal activities. The basic impact, place and role of recognition and counter-recognition in cyberspace are identified. The economic impact in terms of the level of development of cyberspace is also assessed.

Keywords: Cyberspace, information warfare, organized crime.

Introduction

As society develops, a broad range of types of crime is emerging, encompassing both individual and organized crime. Criminal methods, and the ways in which crime is organized, are directly related to the technological development of society. For this reason, crime is evolving and is increasingly shifting its activity to cyberspace, progressing hand-in-hand with the development of information and communication technologies (ICT), as used in the realm of cyberspace, which is a widely understood concept. This applies both to individual crimes and, increasingly, to organized crime as well. Cyberspace has become the perfect environment for committing crimes as well as for enabling new ways in which to run organized crime and manage new forms of competition for influence. This mainly occurs with regard to the impact of information, both on enemy criminal organizations (competing with each other) and on governments and international institutions combating organized crime. Interactions of this nature bear the hallmarks of a conflict or war for influence conducted in cyberspace, aimed at creating a positive image of a criminal organization, misleading the institutions combating crime and destroying potential competition – and all

via the means of information interaction. The scale of this phenomenon will grow as the information society develops and interaction with it will take a variety of forms, both logical and kinetic.

Therefore, it is critically important to identify the forms, methods and impact of organized crime in cyberspace, as well as ways to combat it. There will be conflicts in cyberspace, bearing the hallmarks of war, and characterized by asymmetrically weighted opponents, unlimited reach, unknown consequences, and unidentified objectives on the part of the rival.

Conflicts in cyberspace will differ in character from the well-known conflicts of the past. This follows the commonly used saying that every age has its own war, consistent with the level of technological and social development. Indeed, this can be observed in the ways in which war is conducted and the measures which are taken during that war. Access to information stored, processed and transmitted via cyberspace has given society a new quality of life, making possible various social functions that were mere star-gazing and fantasy in the not-too-distant past. It manifests itself not only in the rapid development of society, but also has a considerable economic dimension, as shown by the reduction in the cost of the functioning of society while accelerating the implementation of this functioning.

On the one hand, these technologies enable the development of new social forms while, on the other, they raise legitimate concerns regarding their use. The best examples of the impact of modern technology on the functioning of society include the Internet blocks put in place in Estonia in 2007 and in Georgia in 2008. This new dimension, namely, cyberspace, will have a huge impact on the functioning of society, the course of future conflicts and the ways in which organized crime functions. The scope and impact of the competition are mere estimates, based on the above-mentioned examples.

The primary aim of this article is to identify possible ways in which organized crime interacts and competes in cyberspace as well as ways in which it can be combated by governments and international institutions.

In terms of the activities of organized crime and its impact on global society, it is important to identify the nature of contemporary conflicts and define the very essence of war because the cyberspace activities of organized criminal groups bear the specific hallmarks of a war for influence and profit maximization. The war itself, as a social phenomenon, in the present terms, is difficult to define. It consists of various factors related to, among other things, the incredible acceleration of global economic development, population growth, and political changes in the international arena. Terms such as *economic war*, *war of information* or *political war* are frequently mentioned. War has become a term often used by various political bodies to express their attitude to the situation. It is the rhetoric of the political arena, focused on exerting a specific social and international impression. The boundary between what war is and what war is not, is difficult to determine, especially in recent times when this term is com-

monly abused by some politicians and experts expounding on the 'global war on terror' or the 'war against organized crime.'

For example, Boleslaw Balcerowicz, a recognized Polish military theorist, believes that contemporary definitions of war reveal a close relationship between politics, the state, the war and the counter-war (also violent) as an instrument of policy.[1] It represents a kind of game between strength, power and the people, or in other terms, intelligence, strength, and a (blind) component. War, as a form of conflict resolution between the warring parties, is characterized by the use of violence, appropriate to the situation, the possession of capabilities and social development. In this regard, the economic and social costs arising from waging war, which must be taken into account by every authority in a democratic society, are important in terms of the functioning of the state. Therefore, the approach to war, including the fight against organized crime, should take into account the ratio of the economic cost of activities to the results achieved, as well as social costs, i.e., the nuisance to society, which plays an increasingly important role. These factors constitute grounds for being aware of the use of cyberspace as a field on which organized crime groups compete, not only perpetrating crime against individual governments and international institutions, but also among themselves. It is also important to pay attention to the ways and methods in which criminal activities of this nature can be combated within cyberspace.

Asymmetry of Information

Asymmetry, indicating a lapse in or lack of symmetry, is reflected in many areas of human activity, including—but not limited to—the level of development of cultural, economic and technological societies. States are trying to move up the international ladder by leveraging economic growth and by using the latest technologies to increase the competitiveness of their economy and further develop their society. One of the indicators of modernity is the existence of IT infrastructure, serving not only as a tool for public access to and exchange of information, but increasingly as an indispensable element of state functions.

Cyberspace is also reflected in normative documents, which define cyberspace in various ways by taking into account purely technical or purely human aspects. In the author's opinion, cyberspace today represents an environment in which individuals and whole societies can both create new forms of relationships, along with new methods of cooperation and functioning. It is a type of space in which we can exist independently from the surrounding environment. The mainstay of cyberspace is information. We can therefore attempt to define cyberspace as a space of cooperation between people using electronic devices for the generation, storage, transmission and processing of information. This

[1] Boleslaw Balcerowicz, *Czym jest współczesna wojna?* http://www.pl.ism.uw.edu.pl/images/stories/Publikacje/ebiblioteka/balcerowiczwspolczesnawoja.doc, accessed January 15, 2016.

definition necessitates a corresponding definition of electronic devices, understood as the elements within IT infrastructure that create an environment for the exchange and processing of information. This environment is the Internet and the other telecommunication networks used to transmit, process, and store information. Generally speaking, and bearing in mind the issues relating to the theory of systems, the Internet is a technical system, creating infrastructure for the transmission, processing and storage of information. Cyberspace is a social system in which the most important element is its users and which is based on the technical system of the Internet and other ICT networks.

Thus, a defined space becomes an arena of positive cooperation, namely, development in the areas of education, society, economy and security, as well as an arena of negative cooperation, in terms of cyber surveillance, cybercrime, cyber terrorism and cyber war. This latter area of cooperation forms part of the activities of organized crime.

The analysis conducted showed that new, previously unknown threats go hand-in-hand with the development of new technologies. In terms of the development of cyberspace, the primary threat seems to be the reliance on technology and the inability to return to the way in which the state functioned prior to the introduction of these technologies. This is confirmed by observations of negative events in the cyber sphere. The degree of dependence on technology will depend on the technological development of the state and on the level of its preparation for potentially harmful phenomena in cyberspace. The more advanced the stage of development, the more vulnerable the functioning of the state and society is in the event of accident or damage to, or destruction of, technologies. Organized crime in cyberspace becomes even more dangerous.

Countries with well-developed ICT infrastructure and sophisticated defense systems for this infrastructure will have an information advantage by comparison to less developed countries. In turn, the lack of adequate defense systems for developed ICT infrastructure can manifest itself in the paralysis of state decision-making organs, and have severe social consequences. On the other hand, states with underdeveloped ICT infrastructure (or even an informal organization of a criminal nature) with mechanisms, procedures and structures able to interact with the IT infrastructure of another country can threaten the foundations of a more developed country, and undermine its economic, political, military and social systems. The modern world is home to a type of information asymmetry.

Possession of the right structures and mechanisms to protect a country's own IT infrastructure and information resources now forms an indispensable element of cyber security and represents the very basis of national security. Another important aspect of the information asymmetry present in the modern world is the possession of the tools, procedures and structures capable of recognizing and incapacitating the opposite side, in the case of organized crime. These two elements map on to defense and attack in the cyber arena and, *inter alia*, will become an indispensable part of the fight against organized crime.

The quality of these elements will affect the course, cost and effect (degree of realization of the objectives) of actions carried out.

From the point of view of information asymmetry, it appears necessary to classify the parties involved in the conflict in terms of the level of development of infrastructure. Included within the first group are countries with well-developed IT infrastructure that are also in possession of network-centric capabilities. This means that they have integrated data communication systems and can share information resources completely. The second group of countries comprises countries with well-developed ICT infrastructure, but who do not possess network-centric capabilities. These countries have fully integrated ICT systems, but do not yet have systems that enable sharing of all the information they possess. This category may include countries that are at the stage of development of ICT infrastructure at which not all their ICT systems have been integrated, meaning that there is no flow of information between the systems. The fourth category of countries includes those countries that do not have IT infrastructure, or those countries in which the level of development of the IT infrastructure is very low, thus prohibiting integration. A separate category covers informal groups, including organized crime networks, which do not have their own national law and which use the IT infrastructure located on the territory of a country (or group of countries) to carry out their business.

Ways of Impact

The use of cyberspace in the form of negative cooperation is nothing but a struggle to gain information superiority over the other side. On the one hand, it comprises the desire to hide information and one's own intentions, to create a false image while striving to obtain information about the intentions of the opposite side; on the other hand, it encompasses ensuring the functionality of one's own information system and paralyzing (incapacitating) the information system of the opposing party.

With such specific purposes in terms of negative cooperation, one should attempt to define information as a factor that determines the course of each conflict. Today, there are a number of different approaches and definitions of the term. For many theorists involved in defining the concept of information, information itself is considered to be the original concept which cannot be defined. Some authors give up on its definition, contenting themselves with its intuitive and colloquial meaning. Interestingly, in terms of the objectives of action in cyberspace, one definition of information was presented by Professor Marian Mazur, the greatest Polish cybernetician, who—in relation to the psychological theory of reflection—states that information is "the relationship between the original and the image of the original."[2] Another definition of information was presented by Piotr Sienkiewicz, who understands information to be

[2] Marian Mazur, *Cybernetic Theory of Autonomous Systems* (Warsaw: PWN, 1966), 35-37.

"a collection of facts, events, features, objects included in such a form that allows the recipient to respond to the situation and take appropriate mental or physical action."[3]

These definitions are focused on the identification of information as a mirror image of observed reality, which does not have to be a reflection of the truth or the facts. Knowledge is built on the basis of this reflection, in conjunction with a number of different factors such as education, experience, the observer's beliefs, and so on. If the resulting picture of reality is, to some degree, far from the truth, then the knowledge created on the basis of it does not guarantee an effective and efficient interaction with reality.

The credibility of the information obtained depends on the quality of the recognition system and the quality of the activities opposing this, or, counter-recognition. These two mutually opposing processes, which compete for information, tend to achieve information superiority over the opponent. The side which gains an advantage in the sphere of information will reach its goal at a lower cost, while maximizing the costs of the opposing party. This system is shown in Figure 1.

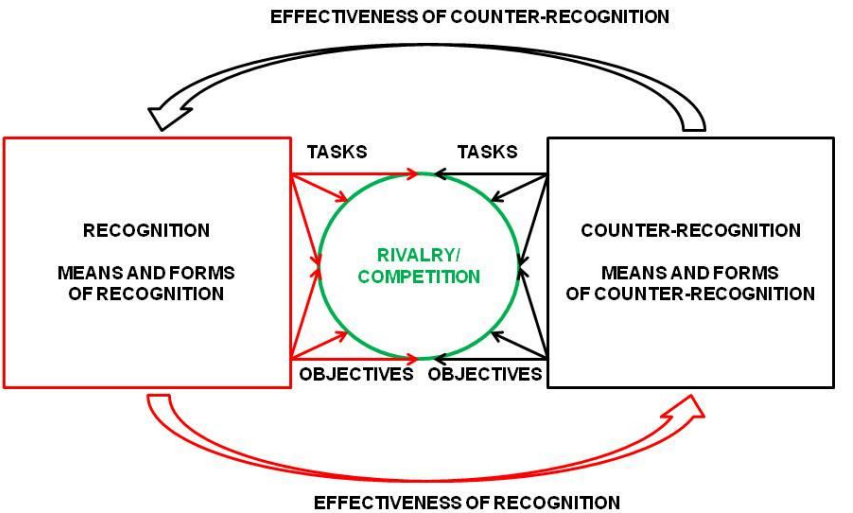

Figure 1: The relationship between recognition and counter-recognition in negative cooperation.

[3] Piotr Sienkiewicz, *Systemy kierowania* (Warsaw, 1989), 128.

When analyzing recognition, it can be noted that this is the process by which we are able to distinguish basic material objects and entities. The subjects in this process are the object of the recognition process and its background, physical information media and any technical devices used by the observer, who is the analyzer and receiver of information. In turn, the subjects of recognition include all the participants involved in this process, including teams of individuals and reconnaissance bodies at various levels in the organization.

As mentioned earlier, the quality of recognition in cyberspace depends on the quality of counter-recognition, which should not only hide intentions (information), but also provide a basic level of protection of information resources. As part of the fight in cyberspace, information counter-recognition should include both active and passive measures.

Active measures in terms of counter-recognition are a way to protect corporate information, carried out by specialized groups using a variety of methods and tools. Its passive (preventative) counterpart involves misleading the opponent by creating a false picture.

Negative cooperation in cyberspace, understood as an information war, requires both offensive and defensive activities which are necessary to achieve information superiority over the rival and achieve one's objectives. Currently, it acts as a prelude to activities conducted outside cyberspace. For this reason, before physical confrontation takes place, whether between criminal groups or criminals and the institutions combating them, the battle is waged on the field of cyberspace, traversing not only the territory of the parties directly involved in the conflict but also the cyberspace of the international community. The battle can either take a slow or a violent course. In the former, the impact on the opposite side will unfold gradually, with no noticeable beginning of the attack, which may go unnoticed or be dismissed as a daily online phenomenon. In turn, the violent attack will be characterized by the high intensity of the cyberspace interaction, and its effects will be felt keenly.

In trying to identify the manner of interaction in cyberspace, it can be broken down into its fundamental stages. The first stage involves developing information superiority by creating a positive image of the parties involved in the conflict. Organized crime depends on concealing a group's true activities and creating a favorable atmosphere for the group to expand its sphere of influence. The next stage is recognizing the opponent's information system (enemy criminal group or state institutions in the fight against organized crime) targeting its components, information resources, procedures and critical infrastructure. Counter-recognition is the stage equivalent to a diagnosis, namely, activities aimed at confusing and misleading the rival and protecting one's own information system. The last stage in this timeline of negative cooperation in cyberspace is the incapacitation of the rival's information system by leveraging the impact of information and, as is likely, physical (kinetic) effects.

The aim of the above steps involved in cyberspace combat is the gaining of information superiority, transitioning to the development and conduct of

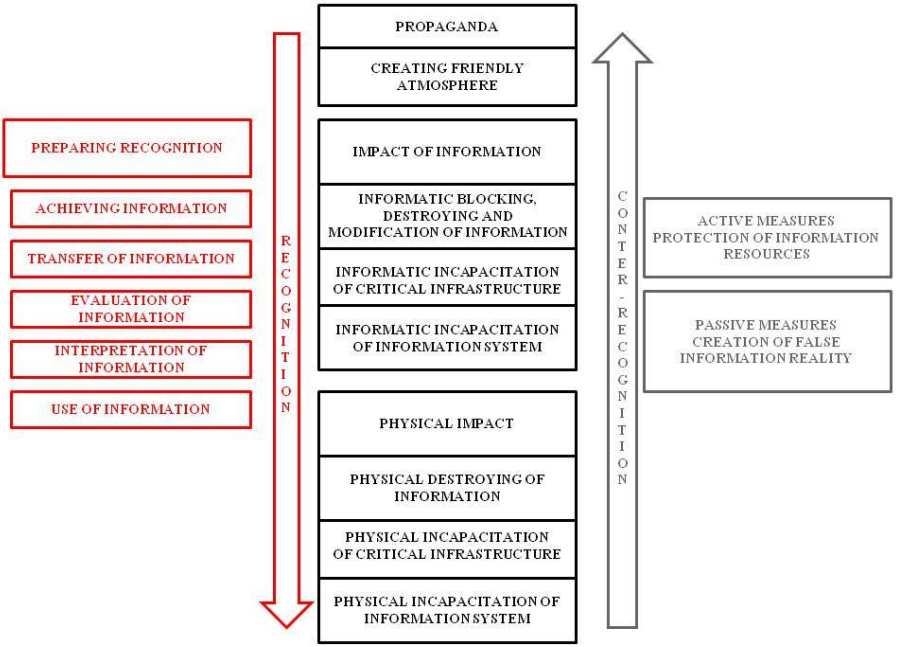

Figure 2: Recognition and counter-recognition in cyberspace.

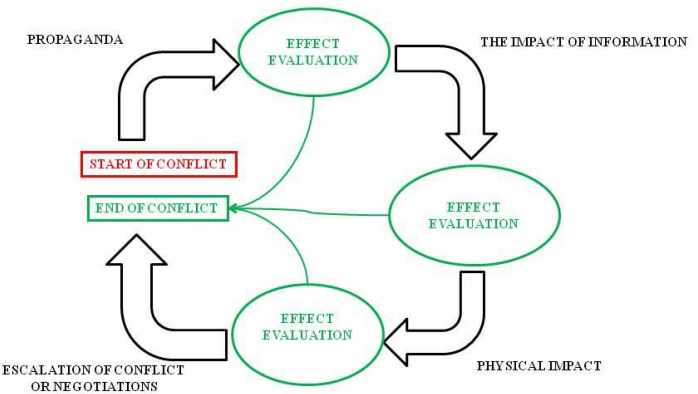

Figure 3: Areas of combat in cyberspace.

criminal activity from a superior position or forcing an opponent into submission as a result of the impact endured in cyberspace. Figures 2 and 3 show the areas in which organized criminal groups might wage war in cyberspace.

Conclusion

This article presents certain aspects of the impact of organized crime in cyberspace. A new dimension of organized crime was revealed, along with its impact on the development and course of potential conflicts conducted for the purpose of gaining influence and profits. Significant phenomena, as observed in the contemporary world, were identified, namely, disparities between the levels of development of individual countries. These manifest themselves, *inter alia*, in the level of development of IT systems and infrastructure associated with a party involved in a conflict, and leads to information asymmetry.

According to the author, warfare in cyberspace and the struggle for information superiority will provide a new form of competition in the international arena, including the fight for influence as pursued by organized crime rings. Its consequences will be severe, impacting not only on the economic sphere, but, primarily, on the social sphere.

Bibliography

Alberts, David S., John J. Garstka, Frederick P. Stein. *Network Centric Warfare*, 2nd Revised Edition. Washington, D.C.: DoD C4ISR Cooperative Research Program, 2000. Available at www.dodccrp.org/files/Alberts_NCW.pdf.

Balcerowicz, Bolesław, *Czym jest współczesna wojna?* Available at http://www.pl.ism.uw.edu.pl/images/stories/Publikacje/ebiblioteka/balcerowiczwspolczesnawoja.doc.

Balcerowicz, Bolesław. "Wojna. Kwestie nie tylko terminologiczne," *Myśl wojskowa* 3 (2003): 53-74.

Balcerowicz, Bolesław. *Polskie wojny*. Available at www.pl.ism.uw.edu.pl/images/stories/Publikacje/ebiblioteka/balcerowiczPOLSKIEWOJNY.doc.

Cebrowski, Arthur K., and John J. Garstka. "Network Centric Warfare: Its Origins and Future," Proceedings Magazine 124, no. 1 (January 1998): 28-35.

Gonzales, Daniel, Michael Johnson, Jimmie McEver, Dennis Leedom, Gina Kingston, and Michael S. Tseng, *Network-Centric Operational Case Study. The Stryker Brigade Combat Team*. Santa Monica, CA: RAND, 2005. Available at http://www.rand.org/pubs/monographs/MG267-1.html.

Kotarbiński, Tadeusz. *Traktat o dobrej robocie*. Wrocław: Ossolineum, 1969.

Mazur, Marian. *Cybernetic Theory of Autonomous Systems*. Warsaw: PWN, 1966.

Munkler, Herfried. *Wojny naszych czasów*. Kraków: Wydawnictwo WAM, 2004.

Sienkiewicz, Piotr. *Systemy kierowania*. Warszawa: Wiedza Powszechna, 1989.

Sun Tzu. *Sztuka wojny*. Warszawa: Przedświt, 1994.

About the author

Colonel Eng. Piotr Dela, Associate Professor, is a graduate of the Faculty of Cybernetics of the Military University of Technology in Warsaw. From the very beginning, his work was focused on the main institutions of the Ministry of National Defense and military education. Since 1998, he has been an academic at the National Defense University of Warsaw. He currently works in the Institute of Security Systems Engineering of the National Security Faculty. Col. Dela is the co-author and co-organizer of a series of military exercises in the field of IT security. He has written over 100 articles, papers, textbooks, scientific papers and monographs. Areas of scientific interest include decision support systems, communication and information systems, information security, cybersecurity. *E-mail*: p.dela@aon.edu.pl.