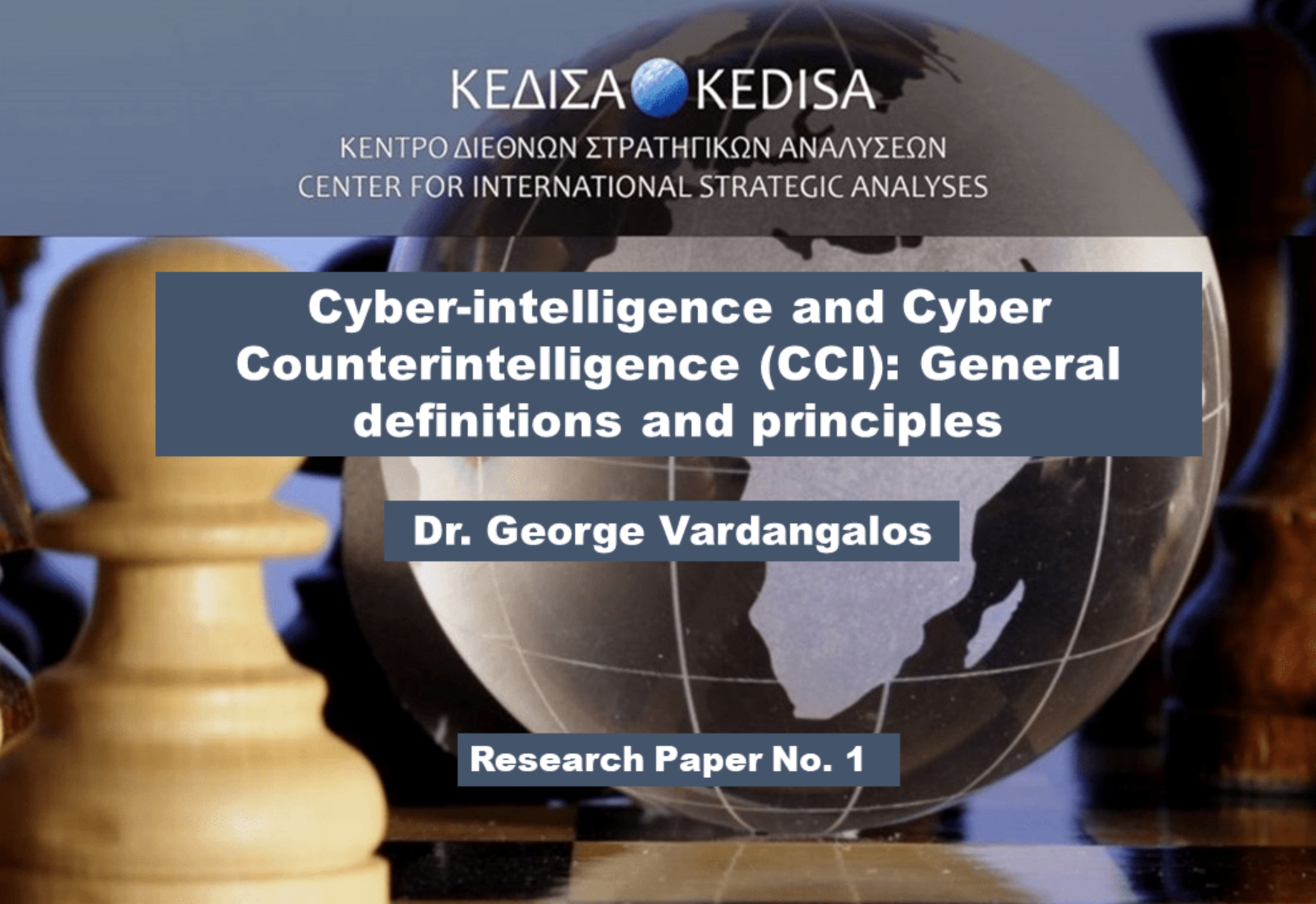

ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ

CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Cyber-intelligence and Cyber Counterintelligence (CCI): General definitions and principles

Dr. George Vardangalos

Research Paper No. 1

ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ
CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Cyber-intelligence and Cyber Counterintelligence (CCI): General definitions and principles

Dr. George Vardangalos
Analyst KEDISA

Research Paper No. 1

What is cyber-intelligence?

It has to be realized that intelligence tactics, techniques, and procedures (TTPs) as well as various types of operations existed long before cyberspace was conceived.

The U.S. Department of Defense (DoD) published a document titled “Joint Publication (JP) 2-0 Joint Intelligence” [1] that serves as a foundation for their understanding and use of intelligence.

In this document the definition of intelligence is**:**

- *The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.*
- *The activities that result in the product.*
- *The organizations engaged in such activities.*

More simplistically, Intelligence is at the same time a product and process from collecting, processing, analyzing, and using information to meet an identified goal.

According to “Cyberspace Operations Concept Capability Plan 2016- 2028” [2] cyberspace is one of the five operational domains; the others are air, land, maritime, and space. These five domains are interdependent. Many researchers emphasize the complexity of the cyber operational domain, the speed in which activity and operations take place, and the supposed inherent advantage of the attacker. Additionally, it is difficult to characterize cyberspace, the meaning of “cyber” domain is changing fast during the last 10 years as the interconnections of the different layers of cyberspace are also increasing. [3]

Therefore, there is no “clear” definition of cyber-intelligence, but in the context of this article, two different definitions will be mentioned. The first one by RSA defines cyber intelligence as “knowledge about cyber adversaries and their methods combined with knowledge about an organization’s security posture against those adversaries and their methods from which situational awareness and/or actionable intelligence is produced. Actionable intelligence is knowledge that enables an organization to make decisions and take action”. [4]

The second definition comes from the Carnegie Mellon Software Engineering Institute and defines cyber intelligence as “the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision-making”. [5]

(Cyber)-intelligence lifecycle

The traditional intelligence lifecycle is adapted and used in cyber intelligence. The intelligence cycle is a circular and repeated process to convert data into intelligence useful to meeting a goal of a user or customer; it has the following steps [6]:

- **Planning and direction** – Determine the requirements and needs of the specific cyber-intelligence effort. Have a defined goal and intentions in order to create appropriately any amount of intelligence out of information.
- **Collection** – Where and how to get the data and information to process. The environment to collect data and information can be honeypots, firewall logs, Intrusion Detection System logs, etc.

Most of the available collection options should be defined in the planning and direction phase so you can make reasonable goals or intelligence needs.

- **Processing and exploitation–** The conversion of collected information into something usable. (How the data is stored; or the actual parsing of data such as converting it to human readable information).
- **Analysis and Production –**taking the data and turning it into an intelligence product. It is achieved through analysis and interpretation and thus is heavily dependent on the analyst. All produced reports should meet a defined intelligence need or goal from the planning and direction phase.
- **Dissemination and Integration –** Supplying the customer or user with the finished intelligence product. If the users cannot access this product or cannot use it then it is useless and does not meet a goal.

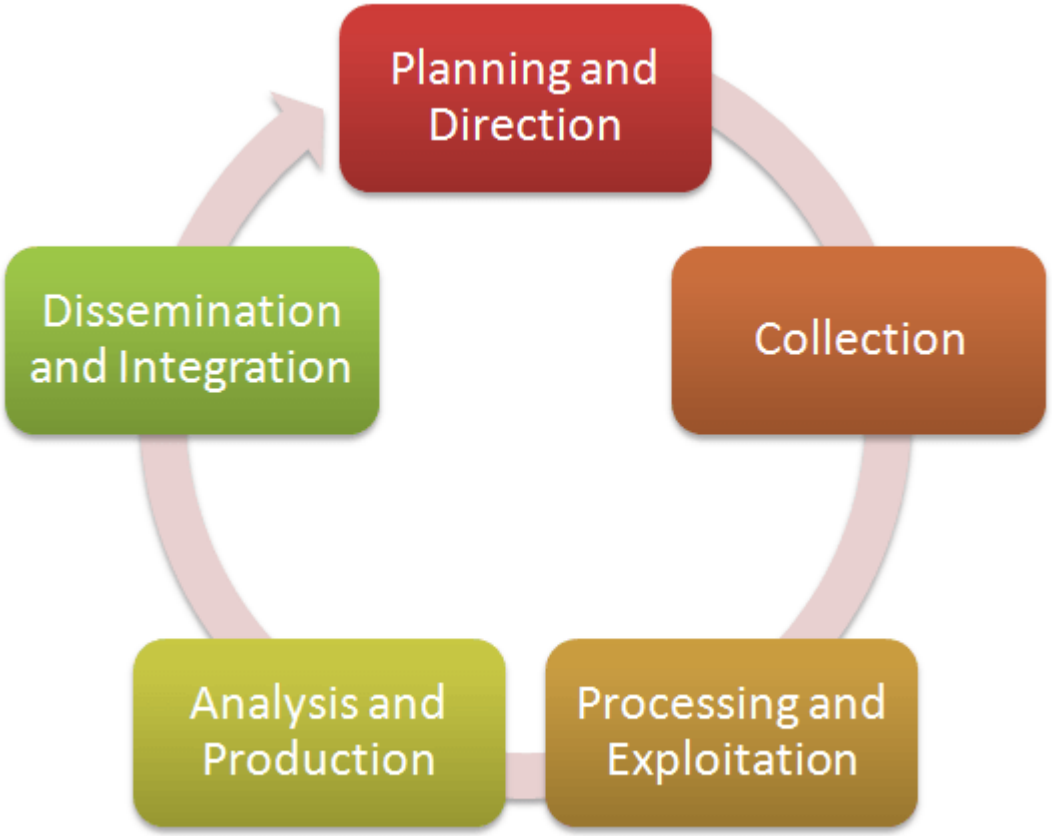

Figure 1: The intelligence cycle

Cyber Intelligence Collection Operations

There are many ways to collect data, by either accessing raw data or getting analysis from other analysts or companies. There is no de-facto standard about where the data comes from and the types of data collected. For an easy-to-understand approach, I will mention the classifications made by *R. M. Lee on this topic [7]:*

According to *Robert M. Lee there are* three types of data collection:

- **Passive** – data collected on networks or information systems you have responsibility over. An example would be analysts capturing internal network traffic, collecting system logs, monitoring internal company forums.
- **Hybrid** – data shared from other networks or information systems or collected from networks designed to entice adversaries (for example, honeypot data, data sharing between external networks)
- **Active** – data obtained from external networks or information systems under the influence of an adversary (for example, adversary account or authentication information, interaction on adversary websites).

Active data collection usually requires analysts to have access to sensitive data. This type of data collection must be done carefully so that the legal and privacy rights of members are protected.

In addition, data could be classified in three types:

- **Raw Data** – unevaluated data collected from a source. This type of data requires extra time to process and analyze it; it should include raw details such as IP addresses, network logs, or network architecture maps.
- **Exploited Data** – data processed and exploited (analyzed) by another analyst, which contains selected raw data. It should include data such as anti-virus/IPS Alerts on your networks, malware reports with samples, technical reports from other networks, Law Enforcement Agency operations, or campaign reports.
- **Production Data** – data finalized into a report meant for dissemination that may include limited or no raw data. It should include data such as government tips, advisories, malware reports without samples, campaign reports without samples.

Cyber Counterintelligence (CCI)

Counter Cyber Intelligence (CCI) is defined as “all efforts made by one intelligence organization to prevent adversaries, enemy intelligence organizations or criminal organizations from gathering and collecting sensitive digital information or intelligence about them via computers, networks and associated equipment” [8] . CCI are measures to identify, penetrate, or neutralize computer operations that use cyber weapons as a means and mechanism to collect information. There is a focus not only on the intrusion, but also on the intent of the intrusion and tradecraft used.

Though there are various definitions for CCI, none of these specifically explicate the relationship between CCI and CI. It is postulated that CI delineates CCI on the following three tiers: [9]

- Applied to the cyber context, CI theory and practice provides a conceptual template for modeling CCI actions in the safeguarding and advancing of cyber interests. Mirroring CI, CCI has offensive and defensive missions that are distinguishable but not separable.
- To be effective, cyber counterintelligence needs to be interlocked with all-field counterintelligence –defensively and offensively. In this sense, CI cements an integrated approach to securing the cyber space. CCI is thus about both the modeling of cyber actions on CI, and the integration of these offensive and defensive actions with conventional CI.

- Effective CI protects and promotes the Intelligence endeavour and business strategy. Since CCI is part of CI, it is also integrated in business strategy and Intelligence.

CCI methods and means can be deployed in offensive and defensive modes: [10]

1. **a) Defensive Cyber Counterintelligence**

Defensive CCI can be thought of as actions taken to identify and counter adversary intrusions before they occur as well as the efforts in identifying and minimizing the threat landscape. In many ways this seems like the role of many cyber security actions: prevent an unauthorized access to facilities and systems, malware intrusions, handling of security incidents and malfunctions, incident investigation and response

A second example of a Defensive CCI action is the performing of *vulnerability assessments and penetration testing***.** The above should be performed with all available information whether it is from OSINT, HUMINT, or technical analysis. *Threat intelligence* is a Defensive CCI type effort. [11]

1. **b) Offensive Cyber Counterintelligence**

Offensive CCI can be thought of as interactions with the adversary to directly collect information about their intelligence collection operations or to deceive them.

Offensive CCI can be leveraged in a number of ways including the use of sock puppets (or virtual agents) on online forums to gather information about adversary intelligence collection operations (capabilities, victims, tactics, etc.), the flipping of adversary operators into double agents to infiltrate the adversary's operation. [12] In addition, honeynets may be configured offensively with the aim of exploiting and deceiving adversaries and display false information to adversial reconnaissance tools, network scanners etc.

First, Middle and Last name
A short bio,
Sex
Age,
Email address(es)
Social networking sites and IDs
City
Country
Profession
Religion
Interests
Connections to other personas you own (a list)
Mother's maiden name
Birthday
Credit card information
Blood type
Height
Weight
Sites where the persona is used
Site roles / responsibilities

Figure 2: Parameters of sock puppets – Tools used like FakeNameGenerator

Conclusion

Cyber intelligence is a complex approach to framing and reacting to cyber adversarial activity. By beginning to define the overall environment and the problem set in manageable operational level, it becomes easier to address the problem. Strategic cyber intelligence should no longer be solely the government's responsibility, but also the commercial sector's one, which owns the vast majority of the cyber infrastructure and the data. They must work together to strengthen cyber intelligence. [13]

In addition, our New Age Risks & Threats demands a holistic approach for Cyber Security:

- **Holistic Approach**: Cyber Security ("online") and "offline" Security must be integrated preferably at the organizational level
- **Culture of Security**: Security awareness & education must focus on the holistic approach, and engage and empower the individual
- **Intelligent Approach**: Intelligence and Risk Analysis must look at cyber security from the outside in, as well of from the inside out.

References

[1] US Department of Defense, Joint Chiefs of Staff, “Joint Intelligence (Joint Publication (JP) 2-0)”, October 2013.

[2] U.S. Army TRADOC, “Cyberspace Operations Concept Capability Plan 2016- 2028”, February 2010.

[3] Clark D., “Characterizing cyberspace: past, present and future,” Massachusetts Institute of Technology CSAIL, March 2010.

[4] Rep. RSA, the Security Division of EMC, “Getting Ahead of Advanced Threats”, Jan. 2012.

[5] SEI Emerging Technology Center, Cyber Intelligence Tradecraft Project, Deliverables, November 2013.

[6] Rocha L., “The Five Steps of Intelligence Cycle”, August 2015.

[7] *Lee R. M., “Cyber Intelligence Collection Operations”, February 2015.*

[8] Carrol, W., “Cyber Counter Intelligence”, Defense Tech, March 2009.

[9] Duvenage, P. C. and von Solms. S.H., “The Case for Cyber Counterintelligence”, 5th Workshop on ICT Uses In Warfare and the Safeguarding of Peace (IWSP’13), Pretoria, South Africa. November 2013.

[10] *Lee R. M., “*Cyber Counterintelligence: From Theory to Practice”, May 2014

[11] Duvenage, P. C. and von Solms. S.H, “Putting Counterintelligence in Cyber Counterintelligence: Back to the Future”, Proceedings of the 13th European Conference on Cyber warfare and Security (ECCWS2014), Piraeus, Greece, July 2014

[12] Bardin, J. “Ten Commandments of Cyber Counterintelligence”, Adapted from Olsen, J. M. “Ten Commandments of Counterintelligence”), CSO Risk. June 2011.

[13] Intelligence and National Security Alliance, Cyber Intelligence Task Force, “Strategic Cyber Intelligence”, March 2014.