gsin

GLOBAL SECURITY AND INTELLIGENCE NOTES

No [illegible] March 2012

BUCSIS
Centre for Security and
Intelligence Studies

! "#$%#$&'$()&*'+#'$,- !) . / / 0 1 0 2 / 0 3 ,

!"#$%&'()*+,-#$(.$/(0,*#)1,*#2213#,-#$/02*0)# $ 1,$4*+*#$4#-0)1*5$

Anastasios-Nikolaos Kanellopoulos
!

Governments, sometimes, appear to lack an adequate appreciation and understanding of the conditions that promote Counterintelligence as a vital pillar of security in state affairs. This may explain why this sector of the Intelligence domain, has not been approached as a holistic security aspect by state actors. Counterintelligence is an integral part of the Intelligence process, carried out by state Intelligence services or, even, by private corporations hired specially for this purpose. Its contribution to state security is vital, since it safeguards the political stability of a state, ensuring its perpetual functioning and internal security, and, also, affects the decision-making process of an adversarial state, through deception operations, that impact its political, economic and military affairs. This article explores the role of Counterintelligence, in a highly competitive and ambiguous

Information collection from a specific subject, while the operational Intelligence environment includes multiple small actions aimed at meeting the needs of a wider operation, such as dealing with an active spy network. Information could be collected from, both, open and closed sources, which are managed according to their classification and the procedure of collection.[13] A closed source is one that provides Information or Intelligence through classified procedures or the material itself has a specific classification, both, in terms of handling by specific employees and of sharing with other services and agencies.[14] Thus, incoming material may be processed and utilized accordingly; however, its further sharing may be subject to certain additional classification or handling restrictions.[15] The United Nations Office on Drugs and Crime (UNODC) describes Information as Òknowledge in raw formÓ that can be used in order to compose Intelligence.[16]

On the contrary, the concept of ÒIntelligenceÓ refers to material that has been formulated, following the collection and processing of one or more pieces of Information.[17] The form and methodology of processing this Information is predetermined in the manuals of the Intelligence services.[18] Intelligence may contain, on a case-by-case basis, Information from open and closed sources, combining and assessing similar Information from many different providers and collaborating services.[19] The UNODC defines Intelligence as Information that Òis capable of being understood, has added value and has been evaluated in context to its source and reliabilityÓ.[20]

Therefore, Information and Intelligence are interrelated factors that support the analytical process, on a different basis. Information is the cornerstone of the analytical products for an Intelligence service. Its effective collection is the foundation for the successful operation of an Intelligence service, as it is the ÒfuelÓ for Intelligence analysis and counteraction. The collection of Information is accomplished with procedures that are related to the role of an Intelligence service and support its objectives and mandates. Intelligence, on the contrary, is the continuation of the Information collection process that results out of its processing, forming the basis for the analytical products produced by the relevant Intelligence department. Intelligence is the outcome of an analytical process, which interprets the facts in order to offer the decision-

Information and Intelligence classification

Incoming Information as well as Intelligence, have specific handling and sharing classification. This is a common procedure in the security and Intelligence services of states and international organizations, adopted through specially designed handling regulations. The necessity derived from the fact that, the collection and management of large volumes of incoming material from different sources, each of them having a different value, need different attention and handling. In addition, the procedure is used.

u(a(ci)33T(u)1 (jia)e(ne)1 i(n)1e(t(u)p3e(u)1 h(e()1-3(01 u(n)a1 ( )-1 (t))-1 (ve1 (e)1 ( )-3 (u)2 (a)1 (te)1 (ri)-1 (a)1 (l)-1 (,)-3 collection of the necessary !nformation, which, after scrutiny and analysis, may be converted into Intelligence that is then used to produce analytical products that are disseminated to other agencies and the decision-makers.[28]

The origin of the IC is found on a theoretical approach proposed by Sherman Kent in 1949. Based on his research, Intelligence refers to the aspects of knowledge, organization and activity, where the Intelligence Cycle includes seven separate phases.[29] Some organizations, as well as other academics, proposed deferent phases for the IC in relation to their strategic and operational needs, connecting the procedure to their internal administrative systems. The CIA describes the IC as a Òprocess of developing raw information into finished intelligence for policymakers to use in decision-makingÓ[30] while the Organization for Security and Cooperation in Europe (OSCE) provides six steps Òused to transform raw data and information into valueadded intelligence aimed for actionÓ[31] The French Division of Intelligence and Fusion Center, approach the IC, as an Intelligence analysis production procedure Òof developing raw information into finished intelligence for consumers, including policymakers, law enf1 (lic)1 o-0.0019 Tc T* r-1 (on1&oc3 (e)1 (n)1 (f1 (lic) (lif1 (lf1 ya)-1 (n) (225Td
The h inini i ormer ion vi (t)-1 (i)-i (e)-s1576uhoier 76ui,

Frocedurss15772he r of ele elr iie rati

The

!

!"#$%%&'&(%&) *+,-*./0123456-*17*81953-2:53-;;:<-56-*89;392-*=TJ -:q[(=TJ -)5 (3)38 1049=TJ -1 (1)-1 (2)-n2-

undermine state security through cooperation with external entities.[39] Every component of CI activities, depends on Information and Intelligence that is processed through the Intelligence Cycle. The CI operational approach varies, depending on the strategic environment in which the Intelligence service operates.[40] The strategic environment relates to qualitative aspects, which affect every country, that condition the operational culture of personnel in the Intelligence Community of each state. However, the theoretical norms of Counterintelligence have a common face in many of these agencies.[41]

Information s ecurity

The first critical task of a CI department is to protect and secure inside information and state secrets.[42] During this process, CI officials are responsible for the establishment of appropriate procedures and security conditions, as well as taking the necessary actions in order to form intangible structures in the Intelligence Community and drastically reduce the chances of any disclosures or leaks.[43] These security frameworks concern, both, the operation of a state and the credibility of the personnel that is involved in sensitive duties.[44] Thus, it is necessary to set up special, internal security procedures, which can lead to the identification of security vulnerabilities regarding infrastructure or procedural gaps and individuals who may pose an Òinsider threatÓ for the Intelligence Community that may potentially cause the leak of information, sources and methods, or analytical material.[45]

Concerning the physical infrastructures, in today's rapidly changing technological environment, CI officers must ensure that proactive cybersecurity measures are in place.[46] In this case, the need for Cyber Counterintelligence arises.[47] This concept describes the process of taking measures to identify, manage and address the actions of foreign intelligence agencies and other actors, that use cutting-edge technologies and cyberspace to access security systems and processes in a targeted state.[48] These foreign attempts seek to obtain Information or analytical material of any form and

[39] Sims and Gerber, Vaults, Mirrors and Masks, 104-112.; Office of the National Counterintelligence Executive (ONCIX), Fundamental Elements of the Counterintelligence Discipline (Washington, DC: ONCIXX

procedures.[56] This process is of the utmost importance for the protection of Information from people that should not have access to or should handle it in specific ways.[57]

In order to ensure personnel credibility, specially designed internal control procedures are implemented.[58] These procedures concern, both, the detailed background check of the so-called ÒprofileÓ of the Intelligence candidate, before taking up Intelligence duties, and the periodic monitoring of his/her official and personal activities.[59] The ÒprofileÓ contains all the factors and activities of a personÕs daily life and social status, that could affect his/her Intelligence duties.[60] This detailed background check includes previous academic, professional and financial activity, family members, close friends and acquaintances, social relationships, personal habits, travel history, and any other Information that could lead to conclusions about the personality, the way of thinking and life perception of the Intelligence candidate.[61] This initial Information, combined with the periodical monitoring of an agentÕs performance and behavior, can contribute to the precautionary detection of security compromises and potential security threats.[62]

Last but not least, beyond checking the reliability of personnel, proper procedures are adopted to espionage tactics and

role, their affiliation to a country or a foreign service as well as the degree of their success at the time of detection.[81] The malicious activities may relate to Information collection but also their direct involvement in operational actions, that aim at influencing and determining the social, political and economic behaviour in the targeted country. The degree of their penetration may be simple, having gained influence over low value personnel, or may have reached high-level officers and executives the role of whom is decisive for the perpetual and proper functioning of the targeted state.

The degree of foreign involvement will significantly determine the operational procedures that will be followed, after their detection. These procedures are vital, as they could create an opportunity for the potential exploitation of the situation, in order to deceive the foreign agency, through the flow of incorrect or directed Information. This technique is often used by Intelligence services, as it can reverse, with relatively little waste of resources, the damage caused by foreign Intelligence activity. At the same time, action is directed against the foreign Intelligence service, which is now receiving incorrect or falsified information leading to the distortion of reality. This manipulation may lead to wrong

!

and directions, aiming at achieving the effective coordination of the national Counterintelligence network.[108] It is important to note that this CI operational culture, must be based on the constant monitoring of the rapidly changing security environment, while adapting to new and emerging technological developments that create new security direct contact and continuous cooperation wi (i)-134 0 Td (?a3ooper)-1 (a$ 0 9.12 -1 ( )]TJ -05c 9.12 f 9.12 f/(

*

*

=).#*)$L.$)*

=).#*K*M)-0N*ABABOP*842;*Q19R4S*T+2-*.57:;3243:15*17*3,-*%-S45-U-*)6-5-*SV*)4;4W@:,4R:*=2190UX*%164;*)-692:3V* +,2-43U*45R*Y:R-2*'-26-03:15UZ*

=).#*A*M[-6 N*ABABOP*\:RS1]'-:P*T+,-*Q:;:342V*45R*)173*'1]-2X*"UU-UU:5<*3,-*64U-*17*#:<-2:4^U*)-692:3V*$5<4<-/-53*:5* Y-U3*"72:64*721/*3,-*'-26-03:15*17*=,454:45*45R*%:S-2:45*'1;:3:64;*45R*"64R-/:6*$;:3-Z*U

=).#*E*MQ42N*ABAOP*"S:<4:;*%96:21U-*_P2T53-;;:<-56-*\4:;92-UP*)9202:U-*"3346`U*45R*+-2212:U"*8U1/04243:a-*84U-*)39RV*"54;VU:D*Z

=).#*F*MQ42N*ABAAOP*G321U*'-32:``1U*45R*Q42:51U*'404:14`-:/P*TbVS2:R*+,2-43U*:5*)/4;;*)343-UX*+,-*84U-*17*3,-* L-09S;:6*17*8V029U*Z *

=).#*> *M@95-*ABAAOP*"54U3WU`1;U1U*!45-;;1019;1UP*T+,-*./0123456-*17*81953-2:53-;<-56-*89;392-*:5*)343-*)-692:3VZ*

****

***

"#$!