OP 99.07

Intelligence and the Pursuit of Security Goals

Nicolas K. Laos[*]

The primary functions of intelligence consist in giving warning of the hostile plans, military or political, of other nations or organizations (espionage) and in research and analysis of information. In fact, the task of research and analysis of information is of the very greatest significance since it provides the means by which a decision-making authority can obtain an accurate picture of the actual state of affairs. For instance, Congressional investigation of the attack on Pearl Harbor shows that, even though the United States had no specific information revealing the Japanese plans in a straightforward manner, all the necessary information about an imminent Japanese attack was available in Washington. Yet, the information was fragmented, and the intelligence officials failed to correlate the odds and ends of information and thus create an accurate picture of reality. The attack on Pearl Harbor is a characteristic example showing the crucial significance of research and analysis of information in the pursuit of security goals.[1]

---

[*] Nicolas K. Laos, after completing his education in mathematics and international relations, lectured at City College (London). Currently, he is a Research Associate at the Royal Institute of International Affairs and a financial advisor.

General Donovan explains that, before you can make a decision, you must get information and then "you've got to evaluate and interpret that information. When you do this, then you have a decision that you feel confident is an informed decision. Government is no different. Government policy, too, must be based upon a tested knowledge of the facts. What facts? The capabilities, the intentions, and the policies of other nations… [Intelligence is] just the careful gathering and interpretation of many bits of evidence."[2] In other words, intelligence must give warning, but also it must supply the information for policy-making.

General Vandenberg, one of the first directors of the Central Intelligence Agency, argues that intelligence consists of a process of building up, piece by piece, a "picture" of what is happening in the world.[3] In particular, the intelligence units of the service departments will provide the military, naval and air "pictures", and the State Department unit the political and sociological "picture". The Central Intelligence Agency will put these and its own original work together to come up with an "over-all picture in a balanced, national intelligence estimate, including all pertinent data."[4]

Additionally, Admiral Hillenkoetter, for three years director of CIA, writes that today's intelligence operator is more likely than not "a researcher, engaged in hard, painstaking work, poring over foreign newspapers and magazines, reference works and similar materials, endlessly putting fact upon fact, until the whole outline appears and the details begin to fill in."[5] An intelligence opera-

tor's job is "to winnow the extraneous data from the vital facts and to set these facts in proper perspective, thereby providing the factual basis for high-level policy decisions affecting our national security."[6] Hence, according to Admiral Hillenkoetter, the role of intelligence becomes one of working a "gigantic jig-saw puzzle" which finally emerges as a picture of what is happening in the world, containing all the relevant facts arranged in their proper relationships to each other. In fact, this "gigantic jigsaw puzzle" analogy provides the criterion which determines what new information is necessary and credible, since the credibility and necessity of new information are partly established by the ease with which the information fills "gaps" in the puzzle.[7]

It should be stressed that the purpose of an intelligence agency is to give warning of future events and to supply the information – analyzed and arranged in a pattern which describes and explains what is happening in the world – on which policy should be based and not policy-making. For example, General Donovan wants an intelligence agency that is central mainly because "intelligence must be independent of the people it serves so that the material it obtains will not be slanted or distorted by the views of the people directing operations."[8]

Cyberwar and Netwar

The information revolution and related organizational innovations have a significant impact on the nature of conflict and the kind of military structures, doctrines and strategies which are necessary. In particular, these imply that communications and intelligence will grow more, (i.e. the emphasis is on C3I.)

and that substantial modifications to military organization and tactics are necessary.

Sproull and Kiesler argue that the "consequences of new technology can be usefully thought of as first-level, or efficiency, effects and second-level, or social system, effects… Advances in networking technologies now make it possible to think of people, as well as databases and processors, as resources on a network… These technologies can change how people spend their time and what and whom they know and care about. The full range of payoffs, and the dilemmas, will come from how the technologies affect how people can think and work together – the second-level effects."[9] Indeed, the technological and the non-technological aspects of the information revolution erode traditional hierarchies, diffuse and redistribute power (often to the benefit of what may be considered minor actors), cross borders and boundaries of any kind, expand the spatial and temporal horizons of the actors, and lead to the substitution of the standard resources, i.e. land, labor and capital, by knowledge.[10]

Cyberwar refers to knowledge-related conflict at the military level, whereas *netwar* refers to societal struggles, i.e. low intensity conflicts by non-state actors such as, for example, terrorists, drug cartels, black market proliferators of weapons of mass destruction, etc.).

Cyberwar refers to: (i) the disruption, if not the destruction, of information and communication systems; (ii) the gathering of every information about the adversary, while keeping the adversary from knowing much about oneself;

and (iii) the turning of the 'balance of information and knowledge' in one's favor (especially if the balance of forces is not), so that less capital and labor are necessary. At the technological level, cyberwar involves diverse technologies for C3I, for intelligence collection, processing and distribution, for tactical communications and identification-friend-or-foe, and for 'smart' weapons systems, as well as electronically blinding, jamming, deceiving, overloading, and intruding into the adversary's information and communication circuits.[11] However, cyberwar does not involve only the implications of the so-called military technology revolution; it is about organization as much as technology.[12]

The increasing importance of C3I matters to the point where dominance in this field alone may yield consistent war-winning advantages to skillful practitioners of cyberwar and the improvement of military training may allow for reductions in the overall size of a state's or an organization's armed forces, especially if it has a clear cyberwar-fighting advantage over its adversaries. Moreover, whereas, traditionally, military operations have been divisible into categories of 'holding and hitting',[13] superior knowledge and control of information may allow for 'hitting without holding'. Finally, the maintenance of a clear cyberwar-fight advantage reduces the significance of nuclear weapons.

Netwar aims at disrupting, damaging or modifying what a target population knows or thinks it knows about itself and the world in general. It may involve public diplomacy measures, subversion – i.e. "all illegal measures short of the use of armed force taken by one section of the people of a country to overthrow those governing the country at the time, or to force them to do things which they do not want to do"[14] (e.g. political and economic pressure, strikes, protest

marches, propaganda and small-scale violence) – insurgency – i.e. "the use of armed force by a section of the people against the government for the purposes mentioned above"[15] – deception of or interference with local media, infiltration of computer networks and databases, and the promotion of dissident or opposition movements across computer networks.

Netwars may occur between the governments of rival states. For instance, the U.S. and the Cuban governments are engaged in a netwar, as manifested by the activities of Radio and TV Marti on the U.S. side and by the activities of pro-Cuban support networks around the world on Castro's side. Additionally, netwar may occur between governments and non-state actors, such as illicit groups and organizations involved in terrorism, drug smuggling, proliferation of weapons of mass destruction, etc. Finally, netwars may occur between rival non-state actors, with governments trying to prevent any damage to the national interests and perhaps supporting one side or another. For instance, in the 1980s and the 1990s, the flow of narcodollars helped fuel inflation in Bolivia, Peru and Colombia as well as financing the narcoterrorism of the Left and the Right.

Intelligence and Foreign Policy

Policy-making in foreign affairs must be based on a formal decision-making process. When decisions are taken at informal sessions, without staff work or follow-up, each interested agency cannot know precisely what decisions have been taken and, even with the best of goodwill, is tempted to interpret the often ambiguous outcome of such meetings in the way most suited to its own precon-

ceptions. And, additionally, there is a high probability of outright error and misunderstanding. Without a more systematic structure, there is little opportunity for conceptual approaches to and consecutive action in foreign policy decision-making. On the other hand, policy-making in foreign affairs should not be characterized by a rigorous formalism in which the policy-making process takes on the character of ad hoc treaties among sovereign departments, as was the case, for instance, during the Eisenhower Administration. However, coherence and precision are essential characteristics of successful policy-making.

Intelligence is a crucial factor in the attempt to achieve the necessary level of coherence and precision in policy-making and to base policy on some basic principles of national interest that transcend any particular Administration and ephemeral personalities. The head of the government relies heavily on the intelligence agency, since the latter supplies early warning to the first; the decision-making authority in foreign affairs must turn to the intelligence agency to learn the facts in a crisis and for analysis of events.

Inherent in the task of ‘warning’ is the prediction of the trends of international events. In fact, intelligence officers have to gather information on developments abroad, to assemble that information into a ‘picture’ of the actual situation under consideration and to project that ‘picture’ into the future. Before they make any major decision in the area of foreign affairs, policy-makers should call on intelligence for the information and an estimate.[16]

A characteristic example of the value of information during wartime is the breaking of the German Enigma code in the Second World War, which gave the Allies important strategic and even tactical advantages. In post-war conflicts, similar information obtained by human intelligence continues to be of crucial significance. For instance, during the Arab-Israeli conflict of 1967, the spy Eli Cohen provided key information on enemy dispositions and was instrumental in making the Israeli pre-emptive strike so devastating. Additionally, the 1973 surprise Arab attack on Israel is a characteristic example of the consequences of the failures of intelligence.

In general, it should be stressed that, since decisions turn on the perception of the consequences of actions which are (best) assessed by the intelligence agency, intelligence on the one hand and policy-making and action on the other should be organizationally, chronologically and functionally coordinated. Intelligence should not be called on only to answer to spot questions; it must be given time for research. Nor should an intelligence agency become a political plum whose director is a puppet of the government and whose task is restricted to the analysis of what has already happened. Finally, an intelligence agency must be set up in such a way that the right kind of people would find it a favorable environment and would feel useful.

Admiral William Owens has analyzed the significance of what he calls a “system of systems”[17] in peace and war. The top layer of this system will orbit in space, the next will be airborne, and the bottom layer will consist of sensors at sea and

above ground. Such a system of systems makes the invasion across the borders of a state equipped with it extremely difficult. In addition, a system of systems is very useful in difficult terrains, such as Bosnia prior to the Dayton accords, where observation is intimately related to engagement. A system of systems helps locate and identify hostile assets, and the broadcasted information guides the attack. If a system of systems works, military operations are more accurate and a substantial saving in logistics is achieved.

Information can facilitate the U.S. military combat interventions whose purpose is to protect and defend other nations and peacekeeping. Moreover, by sending bitstreams to its allies (i.e. information about the battlespace, map data, software for systems integration, simulation and maintenance, etc.), the U.S. can multiply its allies' power and thus encourage them undertake more responsibilities for their security. In other words, the U.S. can fulfill alliance commitments by extending information dominance instead of deploying troops.

Extended information dominance can deter regional aggression. Mutual distrust between states often leads to rearmament, which, in turn, leads to arms races.[18] However, if each state could have credible information about its neighbors' intentions and capabilities and if each state understood that access to U.S. information depended on the maintenance of non-offensive foreign policy, then the level and the rate of rearmament as well as the probability of war could be reduced.

Finally, information plays a crucial role in peacekeeping. For example, the Sinai agreement between Israel and Egypt is reinforced by U.S. sensor systems that warn each side about any offensive movement by the other. Such sensor systems can facilitate peacekeeping in former Yugoslavia, Cyprus, the Golan Heights, the West Bank (monitoring the Palestinian entity in order to safeguard Israel's security), the Aegean Sea (in order to deter aggression between Greece and Turkey), the Persian Gulf, etc.

Intelligence and Low Intensity Operations

The first step of a counter-subversion or counter-insurgency campaign consists in preventing the enemy from achieving control of the civil population and from establishing a successful political organization. For instance, General Grivas writes that his "purpose is to win a moral victory through a process of attrition, by harassing, confusing and finally exasperating the enemy forces with the effect of achieving our aim."[19] In other words, Grivas' campaign consisted of action designed to draw the attention of international opinion to the Cyprus question so as to mobilize international diplomacy. Similarly, the mixture of harassing the government and mobilizing international opinion is the basis of the Palestinian uprising, or *intifada*, in the West Bank of Jordan and the Gaza Strip. In fact, the PLO has managed to be legitimized as a result of a successful campaign that combines diplomacy with crime.

Taking the above-mentioned first step of a counter-subversion or counter-insurgency campaign is an arduous task, since, for a long time, the government

may fail to understand that a significant threat is imminent. Another problem is that in a liberal state, restricting the spread of a political idea is considered to be incompatible with human rights. However, even if early action against those involved in subversion or insurgency may not be possible, preparations for facing a detected threat can and should be made immediately while the institutions involved in counter-subversion or counter-insurgency (such as the army, the police, etc.) should become involved in an advisory capacity. In fact, the government needs to establish a mechanism for dealing with the problem, thus making sure that sound advice will get to the proper people thereby increasing the levels of coordination and efficiency of the government forces.

Apart from the establishment of the above-mentioned mechanism, another important issue is that of the use of law. On the one hand, law can become just another weapon in the government's arsenal, to be manipulated by the government for the disposal of members of the public who threaten the social, economic or political *status quo*. On the other hand, the government may introduce new tough legislation. It is important, though, the law that remains impartial and the executive do not control the judiciary. The second alternative is in accordance not only with the fundamental principles of democracy but also with the government's aim to maintain wide social approval and legitimacy. However, the fact that any violation of law will be treated impartially and the full legal procedure will be followed, safeguarding human and civil rights, may undermine the efficiency of a counter-subversion or counter-insurgency operation, by delaying it. Therefore, the authorities of the forces involved in counter-subversion or counter-insurgency, after consultation with the relevant govern-

ment departments, must inform the top political decision-making authority about the civil and military implications of an operation beforehand. The success of an operation depends on the *early* and *conscious* determination of policy on matters important to the operation's outcome. Moreover, the government must determine the extent of the use of force to be used (either by the police or by the army) in such a way that the operations the adverse effects, on public opinion both at home and abroad, are minimized while, at the same time, guaranteeing the use of sufficient force as well as its application at the right time.

Having dealt with the issues of advice and coordination, the government forces must be prepared for the struggle before their actual deployment. In the pre-violent phase of subversion or an insurgency campaign, the enemy uses propaganda and attempts to organize the people in a certain structure in order to be ready for attack against the government. Hence, the government must counter these moves as follows: (i) by knowing about them in detail, i.e. it must build up an efficient intelligence organization; (ii) by counter-propaganda, i.e. by psychological operations which undermine the appeal of the enemy's message; (iii) by organizing the population in structures similar to those of the enemy when necessary.

It goes without saying that it is difficult to get liberal and democratic states to maintain effective domestic intelligence organizations, especially during periods of peace, because of the economic cost as well as due to the perception that such organizations undermine individual freedom. For this reason, John

McCuen argues that – given that the danger posed by subversion unchecked by good intelligence is far greater than the one posed by the possibility of violations of human rights by domestic intelligence – a liberal and democratic state should possess an efficient intelligence supervised by the elected government[20] Thus, a state is protected from subversion and its citizens do not feel that a domestic intelligence system jeopardizes the freedom of the individual.

Speed is one of the most crucial factors which determine the success of an intelligence organization's operation as well as the success of the preparation of a force to carry out special operations. Subversion or insurgency organizations are particularly vulnerable in the early stages of their campaigns since, at that time, they have not managed to take all necessary security measures and, most probably, they have not managed to cajole or terrorize a large portion of the population. Thus, the quick development of the full potential of the counter-subversion or counter-insurgency forces and the speed of their preparation for operations play a crucial role in the outcome of a struggle.

In times of peace and in the early stages of subversion, the intelligence organization must be able to penetrate the target in order to identify the manner in which it is established, organized and governed as well as the outlook of those employed in it. This end is served better by a small number of accurate and credible sources rather than by a large number of less successful ones. Initially, the target is small and political, and, therefore, a highly specialized and secure organization can achieve the required results.

In peaceful periods, the intelligence organization has to produce what we might call political intelligence, whereas, after the commencement of subversion, in addition to political intelligence, it must produce operational intelligence. The army is involved in the intelligence organization in two ways: first, because the success of its operations relies heavily on the information provided by the intelligence organization, and, second, because it may be necessary for the army to provide individuals to reinforce the intelligence organization or to set up a new intelligence organization.

If a state is with efficient police special forces engaged in fighting subversion or insurgency on its own territories, then there is a strong tendency to use a single intelligence organization based on special branches. With more than one agency, problems stemming from the overlapping of their activities, the production of contradictory information about the same target, the use of the same sources by different organizations and the possible outbreak of war in the underworld among the followers of different factions, exist.

On the other hand, if a state is involved in other states, then a single intelligence organization may not be the best choice or even possible.[21] By setting up a separate organization to deal with the new commitment of providing operational information, the already existing organization is not disrupted by rapid expansion or by the need to devise new methods for getting operational information. Moreover, if a new intelligence organization is set up, it can be manned

by people who are more specialized in the techniques are necessary for dealing with the given issue. However, it must be stressed that, will more than one intelligence organization, their output should be carefully coordinated and analyzed by a committee presided over by a single director of intelligence.

Even though intelligence is of paramount importance in order to defeat the enemy, it often comes in the form of information which cannot immediately enable a police or a military officer to put his men into contact with the enemy. For, even though information collected by intelligence agencies forms the background to operational planning, it may provide material about enemy locations and intentions which is outdated before it can be acted upon by the government forces. Thus, in order to fight subversion and insurgency organizations, it is necessary to collect background information and then to develop it into contact information.

To develop background information into contact information, a system is necessary which involves a commander who collects all the background information he can get. Hetten analyzes it very carefully in order to narrow down the data about the enemy locations and intentions and thus employ his men with a higher probability of success. Because the process of narrowing things down is very difficult, initially, the use of force may aim primarily at getting even more information about the enemy by observation and search and at frightening the enemy. The accumulation of more information by the use of troops enables further deductions, and even further deductions can become possible as a result of

further use of troops, etc. Moreover, the accumulation of information can be sustained by taking prisoners or if letters or equipment falls into the hands of the government forces. The previous process of chain reaction and accumulation of information can bring the enemy to action under favorable circumstances and reveal the enemy's network of support.

In addition, the use of technology facilitates contact information. Technologically advanced intelligence devices play an important role in getting contact information. For instance, information about the enemy can be gathered from monitoring telephones and wireless links, whereas devices designed to improve security are very useful in order to protect the communications of counter-subversion and counter-insurgency forces.

Finally, given that the era of advanced industrialization is characterized by increased mobility of the world population, economic globalization and the emergence of cyberwar and netwar, intelligence networks which act globally are necessary in order to coordinate and supply additional information to the national intelligence agencies. For instance, INTERPOL, the Schengen Treaty and NATO's intelligence contribute to fighting subversion and insurgency globally.

Information Revolution and Emerging Forms of Terrorism

To be able to identify the most efficient anti-terrorist policy, we must, first of all, identify the nature of terrorism. In other words, we must identify the predominant characteristics of terrorism in each segment of space-time. In fact,

the information revolution marks a turning point in the history of terrorism since it strengthens forces that tend to change the nature of terrorism.

The information revolution challenges the assumption that terrorism is predominantly the result of group action. In the super-industrial era, the significance of large, structured organizations as vehicles of terrorism is diminishing. Information technology and chemical/biological weapons are powerful tools in the hands of individuals who want to act on their own or within the framework of a cellular unit of, say, three or four people. Hence, the information revolution reinforces the individualization of terrorism by diffusing power.

To understand the consequences of the above-mentioned diffusion of power and the individualization of terrorism, we must analyze the group dynamics of a terrorist organization and the significance of the idiosyncratic features of a potential terrorist. A terrorist organization which complies with the standard model of a rather large, structured group of people who act pursuing usually well-defined political goals, commits crimes not only in order to weaken its opponent by killing people but also to attract the attention of the public and the international community in general. A characteristic case in point is the PLO. Through time *t* and once a terrorist organization gradually gains wider international recognition (for example, the PLO was granted United Nations observer status in 1974), it tends to become less radical and adopts a more conventional approach toward the establishment (for example, Israel and the PLO negotiated through a secret channel in Norway and on 13 September 1993 signed an interim peace

accord on the White House lawn). Additionally, the more technologically advanced and efficient the anti-terrorist forces are, the less efficient the terrorist organizations become. For, the information revolution facilitates the anti-terrorist forces to identify and learn more about a terrorist organization and thus strike it more effectively and prevent terrorist offences.

However, the previous analysis of the group dynamics of a terrorist organization is not sufficient in order to account for all the aspects of the nature of terrorism. Indeed, the radicalism and the capabilities of a terrorist organization may decline over time, but this need not be the case for individual members of the given organization. Once an individual terrorist is attracted by centrifugal forces to abandon his/her organization and follow an individual path in terrorism because he/she disagrees with the organization on tactical or strategic issues or because he/she wants to satisfy personal ambitions, then the need arises for a different framework of analysis in order to understand the phenomenon of terrorism.[22] A different analytical framework becomes necessary in order to account for terrorism which is the result of insane people or those who want to use terrorism for revenge or as an outlet for their personal frustration (what we might call '*a*-political' terrorism), too; if this is the case, then a terrorist may be indifferent to the attraction of publicity.

Whereas the radicalism of a terrorist organization tends to decline over time, the radicalism of an individual terrorist tends to increase over time. A terrorist who is a member of a terrorist organization struggles, to a certain extent, for

the achievement of the *organization's* goals in order to vindicate his/her participation in it, i.e. his/her behavior obeys the laws of collective behavior, but the achievement of a goal by an individual terrorist is the ultimate foundation of his/her *own self-esteem*. Such an individual has adopted the goals of a terrorist group to which he/she belonged for some time or he/she pursues totally personal goals (e.g. revenge); these goals are clearer and more crystallized in his/her own mind than they would be in a group and the means by which he/she will pursue them are not restricted by any procedure of collective decision-making. Hence, an individual terrorist or a cellular terrorist unit is potentially more unpredictable, flexible and efficient and, hence, more dangerous than a structured terrorist organization.

Alvin Toffler argues that as "interdependency grows, smaller and smaller groups within society achieve greater and greater power for critical disruption. Moreover, as the rate of change speeds up, the length of time in which they can be ignored shrinks to near nothingness."[23] Indeed, as a result of the information revolution, the units of the social system become more and more interdependent, structures and authority relationships last less and less, multiculturalism stresses the rights of any grievance group and fictional 'community'[24] (e.g. the handicapped, the gay community, etc.), and technology diffuses power which allows any unit of the social system to pursue its goals in a violent way (e.g. through use of explosives, electronic warfare, biological warfare, etc.).

Given that the information revolution modifies the nature of terrorism by giving

rise to new forms of terrorism which are added to the previous ones, intelligence must be adjusted to the new reality. In particular, the individualization of terrorism urges the intelligence community to use equally small intelligence units in order to counter individual terrorists or cellular terrorist units. In other words, to counter a flexible and almost unpredictable terrorist or cellular terrorist unit, we need an intelligence unit of equal or proportional size, which will be flexible, able to take and implement decisions quickly and will have sound operational experience and intuition. Thus, the anti-terrorist struggle must be centralized at the strategic level and decentralized at the tactical level. At the tactical level, in particular, anti-terrorist operations should be based on the principle of equal or proportional response; i.e. the intelligence units should try to counter terrorist units by copying their tactical advantages in order to neutralize any tactical advantage that terrorists might have.

As a result of the above-mentioned analysis, we need more political intelligence, safer and more effective intelligence networks and higher levels of information security. To reinforce political intelligence without challenging an individual's request for the protection of his/her civil rights and individual liberties by the government, the intelligence community must make clear that, if the necessary precautionary measures are not taken, public order and the good of life are at stake. Therefore, the government must guarantee civil equality in order to deprive as many people as possible of any political justification of the use of violence. Moreover, as argued above – because, in the cybernetic era, geographical constraints are declining – the fighting of crime becomes a global issue (i.e. it cannot be tackled effectively on a national basis). Hence, it is necessary to

construct credible international intelligence databases that help identify (potential) criminals and prevent them from threatening the public's life and prosperity.

Notes

1.See G.S. Pettee, *The Future of American Secret Intelligence*, (Washington D.C., 1946), p. 7; S.W. Richardson, “Why Were We Caught Napping at Pearl Harbor?," *Saturday Evening Post*, May 24, 1947; W.J. Donovan, “A Central Intelligence Agency: Foreign Policy Must Be Based on Facts," *Vital Speeches*, May 1, 1946.

2. See W.J. Donovan, “A Central Intelligence Agency," p. 446.

3.Testimony of General Hoyt S. Vandenberg, *Hearings Before the Committee on Armed Services*, United States Senate, Eightieth Congress, First Session on S. 758, Part 3 (U.S. Govt. Printing Office), p. 491.

4. *Ibid.*, p. 499.

5. See R.H. Hillenkoetter, “Using the World’s Information Sources," *Army Information Digest* III (11) (1948).

6.*Ibid.*, p. 4.

7.Testimony of General Vandenberg, Hearings on S. 758, p. 498.

8.See W.J. Donovan, “A Central Intelligence Agency," p. 446.

9.See L. Sproull and S. Kiesler, *Connections: New Ways of Working in the Networked Organization*, (Cambridge, Mass.: MIT Press, 1991), pp. 15-16.

10.See T. Stonier, *The Wealth of Information: A Profile of the Post-Industrial Economy*, (London: Thames Methuen, 1983).

11.See C.L. Powell, “Information-Age Warriors”, *Byte*, July 1992; D. Ronfeldt, *Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution*, (Santa Monica: RAND, 1991); A. Toffler, *Powershift: Knowledge, Wealth and Violence at the Edge of the 21st Century*, (New York: Bantam Books, 1990).

12.See T.P. Rona, *Weapon Systems and Information War* (Seattle: Boeing Aerospace Co., 1976); D. Ronfeldt, *Cyberocracy, Cyberspace, and Cyberology*; A. Toffler, *Powershift: Knowledge, Wealth and Violence at the Edge of the 21st Cen-*

tury.

13.A characteristic example is the 1944 battle for Normandy. Field Marshal Montgomery's forces tied down the German Seventh Army and allowed General Patton's Third Army to attack against the German defenses.

14.See F. Kitson, *Low Intensity Operations: Subversion, Insurgency & Peacekeeping,* (London: Faber and Faber, 1971), p. 3.

15.*Ibid.*.

16.See W.J. Donovan, , "A Central Intelligence Agency."

17.See W.A. Owens, "The Emerging System of Systems", *U.S. Naval Institute Proceedings*, May 1995, pp. 35-39.

18.See A.M. Saperstein, "Mathematical Modeling of the Effects of 'Capability' and 'Intent' on the Stability of a Competitive International System", *Synthese,* 100(1994), 359-378.

19.See G. Grivas, *Guerrilla Warfare,* (Longmans, 1964), p. 92.

20.See J. McCuen, *The Art of Counter-Revolutionary War,* (London: Faber and Faber, 1966).

21.According to R. Thomson, in Saigon in 1966, there were no less than seventeen intelligence agencies at work, and, according to J. Paget, ten separate intelligence organizations were operating until Brigadier Cowper re-organized the system in 1965. See R. Thomson, *No Exit from Vietnam,* (Chatto and Windus, 1969); J. Paget, *Last Post: Aden 1964-67,* (Faber and Faber, 1969).

22.For instance, immediately after the end of the American Civil War, the Ku Klux Klan was a powerful terrorist organization, but, by the end of the 20th century, its social impact is of marginal significance as a result of the fact that information technology and intelligence allow the FBI to monitor this organization and prevent it from committing any significant terrorist action. However, the FBI should not just laugh at a colorful organization like the Ku Klux Klan; it should not be oblivious of the danger that a former member or a cellular unit of the Klan may pursue an autonomous and potentially lethal career in terrorism. Similarly, during the 1990s, the PLO gradually reduced its radicalism as a result of the achievement of increasing levels of international legitimacy and because of the international pressures that Arafat faced after his major diplomatic mistake to support Saddam Hussein, who was even condemned by the overriding majority of the Arab states and was defeated

in the Gulf War in 1991; yet, certain individual members of the PLO do not approve of the new mainstream political choices of the PLO (accommodation with Israel) and consist potential agents of havoc.

23.See A. Toffler, *The Future Shock*, (New York: Bantam Books, 1990), p. 477.

24.For instance, in the United States, there are hundreds of religious or quasi-religious sects. By restricting intelligence to the monitoring of these sects as such, we can prevent them from using terrorism, at least on a large scale. Yet, we are doing almost nothing about the possibility of a (former) member or a small number of (former) members of any of those sects resorting to terrorism because of zeal, temperament, frustration, tactical choice, etc.

Scenario simulation of the malicious use of artificial intelligence and protection against related threats requires broad international cooperation and the creation of special national andâ€¦Â Eighty-seven percent of security experts polled by Neustar agree that AI is important for protecting their company. However, the majority (82 percent) of experts are also concerned about possible MUAI against their company (see: NeuStar, 2018). According to the 2018 U.S. Government Accountability Office (GAO) report, AI poses the main threat to U.S. national security among dual-use technologies (U.S. Government Accountability Office (GAO) 2018, p. 8). The aim of this study is to identify the range and level of AI-based threats to IPS. Indeed, the pursuit of any challenging goal often involves actively analyzing tasks and then planning, self-monitoring, and revising strategies (1 â‡“ â‡“ â‡“ â€“ 5). Such strategic behaviors are typically referred to as metacognitive strategies, because they require taking a perspective on oneself and oneâ€™s tactics (6 â‡“ â€“ 8). The use of metacognitive strategies is associated with greater goal commitment, progress, and achievement across important domains of lifeâ€”including academic goals (9 , 10), health and fitness goals (11 â‡“ â€“ 13), and challenging personal goals more generally (14 â‡“ â‡“ â€“ 17...Â We present the results of three studies: two field surveys of people pursuing important life goals and an experimental laboratory study in which a strategic mindset was induced. Congressional Research Service. Artificial Intelligence and National Security. Contents. Introduction .Â The DIB instead defines artificial intelligence as â€œa variety of information processing techniques and technologies used to perform a goal-oriented task and the means to reason in pursuit of that task.â€ 8 Executive Office of the President, National Science and Technology Council, Committee on Technology, Preparing for the Future of Artificial Intelligence, October 12, 2016, p. 6, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.