Cyber, Intelligence, and Security

Volume 1 | No. 1 | January 2017

Jointness in Intelligence Organizations: Theory Put into Practice
Kobi Michael, David Siman-Tov, and Oren Yoeli

The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking
Omry Haizler

Lessons Learned from the "Viral Caliphate": Viral Effect as a New PSYOPS Tool?
Miron Lakomy

An Intelligence Civil War: "HUMINT" vs. "TECHINT"
Matthew Crosston and Frank Valli

Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations
Gabi Siboni and Ido Sivan-Sevilla

Artificial Intelligence in Cybersecurity
Nadine Wirkuttis and Hadas Klein

Pedal to the Metal? The Race to Develop Secure Autonomous Cars
Andrew Tabas

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Cyber, Intelligence, and Security

Volume 1 | No. 1 | January 2017

Contents

Editor's Foreword | 3

Jointness in Intelligence Organizations: Theory Put into Practice | 5
Kobi Michael, David Siman-Tov, and Oren Yoeli

The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking | 31
Omry Haizler

Lessons Learned from the "Viral Caliphate": Viral Effect as a New PSYOPS Tool? | 47
Miron Lakomy

An Intelligence Civil War: "HUMINT" vs. "TECHINT" | 67
Matthew Crosston and Frank Valli

Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations | 83
Gabi Siboni and Ido Sivan-Sevilla

Artificial Intelligence in Cybersecurity | 103
Nadine Wirkuttis and Hadas Klein

Pedal to the Metal? The Race to Develop Secure Autonomous Cars | 121
Andrew Tabas

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

Cyber, Intelligence, and Security

The purpose of *Cyber, Intelligence, and Security* is to stimulate and enrich the public debate on related issues.

Cyber, Intelligence, and Security is a refereed journal published three times a year within the framework of the Cyber Security Program at the Institute for National Security Studies. Articles are written by INSS researchers and guest contributors. The views presented here are those of the authors alone.

The Institute for National Security Studies is a public benefit company.

Graphic Design: Michal Semo-Kovetz, Yael Bieber, Tel Aviv University Graphic Design Studio
Printing: Elinir

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 6997556 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

Cyber, Intelligence, and Security is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

ISSN 2519-6677 (print) • E-ISSN 2519-6685 (online)

Editor's Foreword

Dear Readers,

The periodical *Cyberspace, Intelligence, and Security* is proud to present its first issue. It is a direct continuation of *Military and Strategic Affairs*, which the Institute for National Security Studies has published for the last eight years. The new journal is aimed at writers and readers interested or working in the many fields of cyberspace, including academia, policymaking and government, the army, intelligence agencies, economics, law, and, of course, those who are developing and providing solutions to cyberspace problems, as well as the parties in industry who represent the customers of those solutions.

The new journal will deal with a range of topics, including global policy and strategy in cyberspace, regulation of cyberspace, safeguarding national resilience in cyberspace, and defense of critical national infrastructures. The journal will also devote space to topics related to cyber-force construction, such as the human resources, means of warfare, doctrine, organization, training, and command, as well as aspects of defensive and offensive cyberwar.

The journal will invite experts to contribute articles in legal and ethical issues, privacy protection, in addition to relations between states and the global technological giants of cyberspace. Specialists will be called upon to write about strategic and military thought, the deployment of military force in cyberspace, propaganda operations, analysis of cyber incidents and their ramifications, as well as the balance of deterrence, analysis of cyberthreats and risks, intelligence, information sharing, and public-private partnerships aimed at improving cyber defense. Technological experts will be encouraged to write about technological developments, case studies, research methods, and the development of processes connected to cyberspace.

A call for papers and writing instructions will be appended to every issue of the journal and will be available at the INSS website.

I hope you will find this journal an important forum for learning and developing knowledge about cyberspace, intelligence, and security.

Dr. Gabi Siboni

Jointness in Intelligence Organizations: Theory Put into Practice

Kobi Michael, David Siman-Tov, and Oren Yoeli

Jointness—a concept popular in recent decades in military, intelligence, and civilian systems—represents a change in the way organizations function in a complex and challenging environment, which is characterized by a networked structure, or multiple connections among various entities. The most striking difference between cooperation and jointness is the process of fusion, which is typical of jointness. While cooperation preserves distinct organizational settings, authority, and areas of responsibility, in jointness we see new organizational formats, which represent a synergy that is greater than the sum of all the existing capabilities.

This essay focuses on jointness in intelligence. New ways of thinking over the past years have led to the breakdown of the compartmentalizing of intelligence organizations and have given rise to models of jointness within intelligence organizations, military forces, and civilian entities so that they can carry out complex missions. This essay surveys the theoretical and practical development of the concept of jointness and presents four archetypes of jointness, based on several Israeli and American case histories. These case histories indicate that jointness has not always been applied accurately. The success of jointness depends upon several essential components that may be defined as its ecology. The most prominent is organizational freedom, which provides the space where it is possible and, indeed, recommended to provide autonomy to

Dr. Kobi Michael is a senior research fellow at INSS. David Siman-Tov is a research fellow at INSS. Oren Yoeli is an intern at INSS.

various working echelons; this autonomy allows for flexibility and creativity even if it deviates from familiar modes of action.

Keywords: jointness, the intelligence community, intel, learning processes

Introduction

The concept of jointness, popular in recent decades in military, intelligence, and civilian systems, represents a change in the way organizations operate in a complex and challenging environment. This environment is characterized by a networked structure, that is, multiple connections among entities. Jointness is distinguished from cooperation by the process of fusion. While cooperation preserves distinct organizational settings, authority, and areas of responsibility, in contrast, the process of fusion in jointness creates new organizational formats and synergy that is greater than the sum of all the existing capabilities. Generally speaking, organizations shy away from jointness; yet in a reality characterized by crises and competition, in which organizations find themselves threatened and vulnerable to fail, their inability to produce an effective response to the threats and challenges ultimately strengthens their willingness to engage in jointness.

This essay focuses on jointness in intelligence, having developed as new approaches collapsed the boundaries and separation between intelligence organizations, which—alongside historical rivalries over prestige and competitiveness—had been the hallmark of their relations in the past. These new approaches have also led to the development of models of jointness between intelligence organizations and the military, so that they can carry out complex missions, and also between organizations in the civilian sector. This essay addresses the concept of jointness and seeks to answer the following questions: What is jointness and what led to the need for it? What are the interrelations between the features of jointness? What are the conditions for and obstacles to realizing jointness? How is jointness manifested in the intelligence community, and what are the various jointness models in this world? Examining jointness in its broader context, the essay surveys its development by the American security establishment, its penetration of the civilian corporate world, and its rebound effect on the military and intelligence community. Highlighting the positions of several prominent

researchers on the concept, the essay will seek to expand upon the existing theoretical debate about jointness. Finally, the essay describes and analyzes various models of jointness in the intelligence community—specifically in contexts requiring the use of force—especially in the United States and, in a more limited way, in Israel, in an effort to understand if jointness in the intelligence community is distinctive.

The Development of the Concept of Jointness

The Military

The idea of jointness developed in the American defense establishment in the late 1970s.[1] In the 1980s, the term "jointness" was coined to describe actions, operations, and organizations in which entities belonging to two or more branches of the armed forces took part.[2] Until the 1980s, the command structure of the US military forces was split among five branches, each completely independent in terms of developing doctrine, manpower, and equipment. Battles over budgets took place among the branches, often leading to irrational financial allocations based on size of a particular branch and also to an increase in the overall defense spending.[3] If one branch experienced a problem of resources, it would prefer to handle it by lobbying Congress rather than by cooperating and using existing resources already developed in a different branch.[4]

In 1986, the Goldwater-Nichols Department of Defense Reorganization Act was passed to resolve the difficulties described above.[5] The act brought sweeping changes to the command structure of the US military by strengthening the concept of jointness; the authority and responsibility for force construction was transferred from the branch commanders to the joint chiefs of staff, and geographical commands and the Special Forces command were established. In 1991, the first US military doctrine referring in a detailed and comprehensive manner to jointness was issued, in conjunction with the implementation of the Goldwater-Nichols Act.[6] The doctrine set out guidelines for the armed forces on applying jointness in a variety of ways in order to attain optimal effectiveness.[7] The publication and implementation of the doctrine led to the establishment of several research centers, which developed joint strategies, battle plans, and training. The first war in Iraq, however, highlighted the deficiencies of jointness among the various forces, revealing the gaps between the written doctrines that stressed separate activity and the interfaces that

required a high degree of jointness and, as a result, catalyzed the development of cooperative doctrines that promoted the jointness approach. [8]

The Civilian Sphere

Several years after the development of jointness in the American military, the concept gained acceptance within the civilian and corporate spheres. Changes in management and information technologies led to the development of important theories and applications. The cyberspace revolution enabled businesses to harness advanced computer applications for their needs, speed up processing methods, cut costs, and make information and knowledge accessible to all. At the same time, the acceleration of R&D processes and trade and cooperation among organizations and nations contributed to the declining status of the large business outfits, which were managed in a traditional, hierarchical, and centralized fashion and to the increasing prestige of the more agile and dynamic businesses, characterized by small staffs and independent divisions that manage networks of relationships. The traditional structure typical of organizations for most of the twentieth century gradually made way for a flatter, more decentralized, networked and dynamic model, stressing its many intersecting relations.[9]

The most successful companies were the most cooperative ones; a growing segment of business activity around the world is now carried out cooperatively within an organization, as well as between organizations. Processes of manufacturing and development in many industries (technology, marketing, biomedicine, and more) have become increasingly complex, making a lone organization's attempt to handle these processes independently virtually impossible. For example, the development of information systems at present cannot be carried out as an independent process. Competing companies prefer to incorporate external services in their products instead of engaging in independent development, which would require them to meet constantly changing standards.[10]

Developments in the Theory of Jointness

Zvi Lanir, who worked on developing the notion of jointness in military organizations, defined it as "creating a new systemic capability based on the fusion of the unique assets of the different entities and evincing a deeper connection than coordination or cooperation."[11] Lanir classifies

joint activities in a hierarchic manner according to the quality and depth of systemic influence that they achieve within the military context. According to Lanir, it is necessary to distinguish between the terms "coordination," "cooperation," and "jointness," where each interface characterizes a different level of relationship between entities. Lanir defines "coordination" as "a level of interface allowing [organizations] to attain systemic **efficiency** by a standardization of process," such as coordination of time, location, and intensity between a pinning force and a strike force during battle. Lanir ranks cooperation one rung above coordination. He argues that in order to attain systemic effectiveness (relevance), it is not enough to engage in coordinated systemic thinking. While it allows forces to act efficiently, it does not guarantee the desired effect vis-à-vis the enemy. Every campaign has its own unique features, and every enemy requires unique systemic understanding. "Cooperative systemic thinking" represents the interface of cooperation during which the rationale of the opponent's system is conceptualized.

Lanir places jointness above both coordination and cooperation.[12] Lanir explains that the objective of jointness is to ensure that the systemic effectiveness will continue even under changing circumstances; the relevance of a system can be maintained only if the system is dynamic, and if all the echelons of the different entities are involved in developing knowledge. The new knowledge is created in the encounter between the different entities and results in ongoing organizational transformation. The knowledge is created in the "no-man's cognitive zone," the vacuous space outside of the domain that a single entity can encompass cognitively and exclusively. Lanir refers to the knowledge created in this zone as "joint systemic thinking."[13]

Efron Razi and Pinhas Yehezkeli favor the terms "inter-system cooperation" and "cooperative activity."[14] They claim that jointness is an expression of a degree of organizational freedom that creates a space where it is possible—even recommended—to deviate from familiar procedures, regulations, and operational patterns. This freedom is crucial because in a dynamic, rapidly changing environment, every organization must quickly develop and acquire knowledge. Their claim is that a significant amount of knowledge is created in the interstices between organizations as a result of their interrelations; in order to access this knowledge and develop it, organizations must cooperate with one another.[15] Knowledge may be created in any one of the organization's

echelons; a good flow of information enables the organization to construct processes from the bottom-up rather than being the result of centralized planning from the top-down.

The ideas described above currently shape the perception of jointness in both the US military and the Israel Defense Forces (IDF), and constitute a central component of their approaches. This is particularly true of the US army, which since the early 1990s, has perceived jointness as fundamental to its strategy,[16] while distinguishing between the concept's dimensions and its implementation.[17] Similarly, the IDF distinguishes between jointness as an action or a process resulting from an action and jointness as a concept and as part of organizational culture.[18]

The Dimensions and Stages of Jointness

Jointness is fundamentally a process of continuous learning, and has two major dimensions: the cognitive and the organizational. Jointness takes place in three stages: design, planning, and implementation.[19] The literature tends to distinguish between two main types of learning: causal learning, occurring when new information leads to a change in means and methods; and diagnostic learning, which stems from understanding the tension between values and concepts and results in changes both in the objectives as well as the means of attaining them. Causal learning may also be defined as tactical learning, characterized by adapting and adjusting, whereas diagnostic learning can also be defined as strategic learning, which at its core is a restructured view of reality. In cognitive terms, tactical learning can be seen as an update of existing cognitive structures, resulting in adaptation and adjustment, and strategic learning can be perceived as a change in cognitive structures and their expansion, leading to a change in attitudes and beliefs.[20]

At the basis of the strategic learning process is the concept of "design" as an abstract cognitive process in which the conceptual framework is formulated. At the design stage, existing paradigms are challenged, updated or replaced, and a new vision is formed. The design stage rests on a vision that relates to answering the question, "What do we want to design?" It relates to making decisions and setting a general direction that provides meaning to the process. The vision is seemingly disconnected from the material or practical terrain, which is limited to a fixed total of resources,

and it challenges the organization to think about solutions that transcend these limitations.

Cognition is both a stage of jointness as well as an output (such as organizational understanding) within a wide-reaching organizational process. It is also an outcome of cognitive jointness, in the sense of jointness at the stage of formulating and designing a concept, such as cognitive structuring to interpret reality. Therefore, it would be correct to conceptualize cognition as "cognitive jointness." Cognitive jointness is manifested by joint interfaces and shared thought processes among directors of organizations, who analyze and rethink the challenges that their organizations face and also define shared values. This encounter between organizations abuts upon the inter-organizational space, allowing for the creation of new knowledge in the areas outside the organizational zones of thought (the so-called "no-man's cognitive zones"). Cognition at the design stage occurs by means of diagnostic-strategic learning processes and consists of challenging existing paradigms, bringing them up to date, or replacing them.

In contrast to cognitive jointness, organizational jointness is manifested by shared interfaces and cooperative work among organizations. It includes shared organizational structures, working processes, and the organizational climate ("ecology"), which allow several organizations or frameworks to operate in a synchronized manner and maximize their capabilities—creating a whole that is greater than the sum of its parts—and concurrently helping to promote shared objectives. Organizational jointness is also needed for force building in terms of training personnel and creating organizational infrastructures that efficiently maximize resources and capabilities as a fixed and systematic method for confronting complex challenges. Organizational jointness is expressed more prominently at the planning stage within already existing paradigms that were conceptualized during the design stage. Learning at this stage is simple rather than complex, and it consists of incorporating new information into existing patterns of thinking.

Organizational jointness enables organizations to identify the changes needed within the organizations themselves. These changes may lead to the establishment, dismantling or merger of organizational structures, new job definitions, or new professional ways of looking at things, which may affect the work of existing position holders, as well as defining the components needed to create a joint ecology. Organizational jointness should also include

the implementation stage, which is formulated during the planning stage. The implementation stage is essential to organizational jointness as it is a real test of the organizations in dealing with challenges. During the final stage, the learning process is simple learning, and consists of adapting plans, means, or organizational aspects due to an expected challenge and on the basis of an existing paradigm or concept.

Diagram 1 below describes the dimensions of jointness (cognitive and organizational) as they are manifested at each of the different stages (design, planning, and implementation), while relating to the process of learning at each stage. Cognitive jointness is realized at the design stage, whereas organizational jointness is required throughout all of the stages.

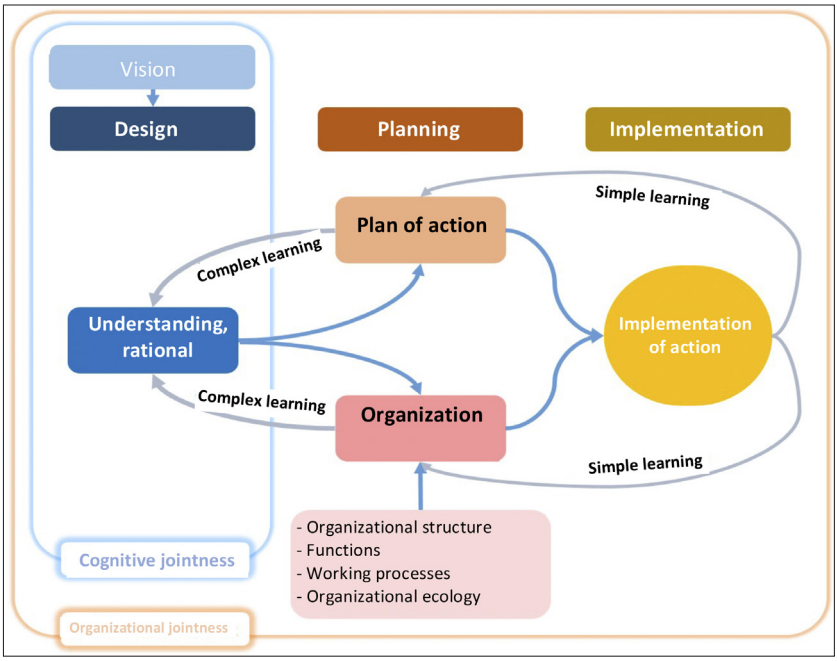

Diagram 1: Jointness as a Learning Process—Dimensions and Stages

As Diagram 1 demonstrates, each stage of jointness generates processes of learning, which allow the realization of the next stage. The final stage of jointness—implementation—is the stage where we can expect to encounter all the problems and challenges. During the final stage, the process of simple learning leads to changing plans, means, or organizational aspects, while

the process of complex learning is needed for much greater problems or challenges, and enables the broader conceptual framework to be reexamined.

Transition from Crisis to the Relevance and Importance of the Organizational Ecology

Jointness may be framed as a process that begins with a crisis; progresses into a conceptual, organizational, and operational development; and leads to improving the organization's relevance in facing problems and challenges in its field. The success of the process also depends on the organization's ecology and environment.

First Stage: Crisis

Crises are the factor that generate organizational processes allowing for the development of jointness as a concept and method of action. The literature defines a crisis as a situation in which a change appears as the result of a sudden event, a sharp change in trend, direction or time. In such a case, an organization needs to reassess the situation; in other words, it needs to reconsider the threats, values, and objectives of the players involved. The change may lie in the internal or external environment, and the threat may be aimed at the organization's highly prioritized objectives or at its basic values.[21] At the beginning of the crisis, the organization manifests a kind of "strategic helplessness," expressing the gap between the organization's relevance and the environment's challenges; that is, the organization expresses its inability to cope with new problems and formulate responses to challenges, given the organization's existing understanding, resources, and capabilities.[22]

Second Stage: Systemic Learning

After recognizing a crisis or the desire to avoid an impending crisis, the organization needs to undertake complex learning processes in order to form the conceptual framework so that it can address the crisis; simple learning processes, designed to allow organizations to adjust action methods based on its present knowledge, are insufficient. When several parties from a number of organizations jointly carry out thinking and learning processes, they realize that the bases of knowledge and paradigms of each organization are insufficient to develop significant insights; this realization can be defined as cognitive jointness. The complex learning process reexamines

the organization, its objectives, the impact it seeks, and the environment in which it operates. One possible means of resolving the ongoing crisis is through organizational jointness, although it is not the only means. In order to promote jointness as a solution, the organizations must recognize jointness as having the potential to provide a mutual reward that is greater than the one produced by separate, individual actions.

Third Stage: Organizational Processes and Ecology

The success of the processes and plan of action that are based on new insights and knowledge are affected by various conditions of the organizational and inter-organizational ecology, including working norms, organizational dynamics, trust among the players, and the extent of autonomy given to the various echelons. Although the incubation processes of the organizational ecology can begin from the bottom-up, its completion and institutionalization must take place from the top-down. Without the support, encouragement, and permission of the organization's management, it is impossible to reshape an organization's ecology.

Jointness is feasible only when the information flows freely between and within organizations. Therefore, the management must provide staff with the autonomy to develop joint interfaces and allow the flow of open and free information in the inter-organizational space. The sides participating in the joint interface will be willing to take risks if they expect positive behavior from the other participants; trust is a function of expectation and of the willingness to take risk.[23] In a situation in which the sides do not have any shared history, they will have no idea what to expect of the other party, and the starting point for their relationship will be neutral. Such a situation requires the gradual building of trust by means of empowering and rewarding positive behaviors.

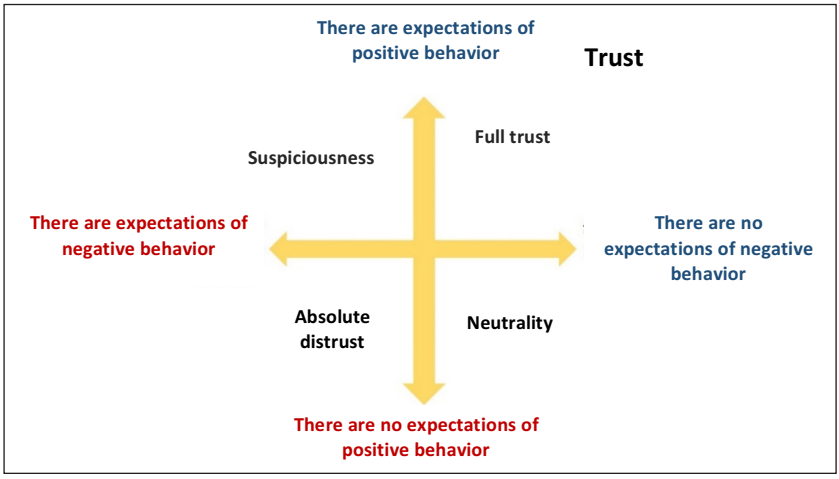

Diagram 2: Trust as a Function of Expectations[24]

Jointness requires working norms and a supportive environment for information sharing, relationship development, and shared processes in which several parties divide the burden of work. The extent of autonomy among employees operating on behalf of an organization in a shared setting affects their awareness of jointness; experience proves that when employees enjoy autonomy it is easier to work together and to build a working environment of mutual trust.[25] In addition, jointness requires that organizations to some extent forgo their original identity and create a new professional identity oriented toward the shared mission. Therefore, in addition to the advantages of being part of a networked association when facing challenges, the new network should avoid alienating individuals from their mother organizations, which employ them and provide them with training, advancement, and professional identities.

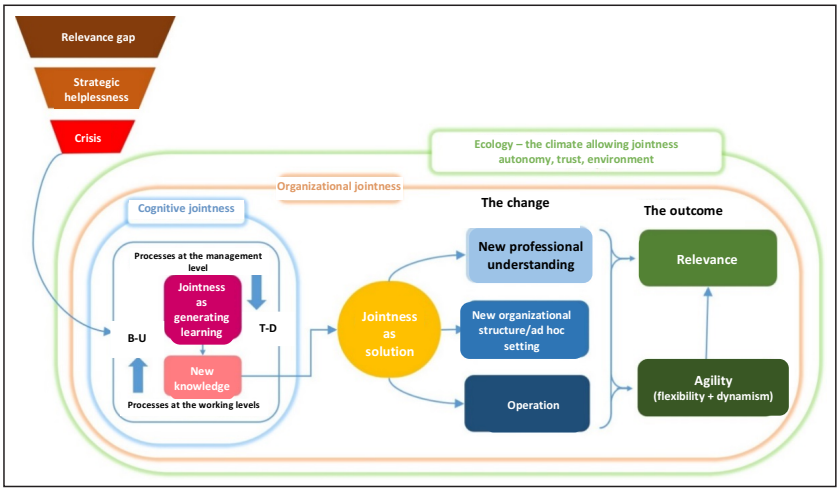

Diagram 3: The Jointness Process—From Crisis to Relevance

Jointness in Intelligence Organizations

The development of jointness in intelligence organizations was influenced by similar processes taking place in the military and the business world, as well as by technological transformations and accompanying changes in intelligence. For example, Itai Brun, who served as the head of the research division in Israel's Military Intelligence Directorate, describes these changes as follows: "In this day and age, the centrality of information technology is striking . . . In such a world, one can gather intelligence of a quantity and quality impossible to gather in the past, then analyze and process it in time constants that were equally impossible . . . The new world is brimming over with information, leading to competition with other information and knowledge providers and revealing weaknesses."[26]

Changes in the technological environment and intelligence challenges have transformed the nature of intelligence work and the outputs now expected. Intelligence organizations must now surveil disappearing targets and incriminate them, and follow processes that lack prior planning or even a clear aim as defined by decision makers.[27] Similarly, the intelligence community is expected to handle incidents in a shorter amount of time (for example, as a result of the use high-trajectory weapons, which do not require any special preparation), while the information revolution has compelled

intelligence personnel to handle a much greater volume of information and knowledge than it did in the past.[28] According to a senior member of the Israeli intelligence community speaking in a closed forum, the Israeli intelligence community has undergone a change of consciousness. In this context, the intelligence community has integrated several organizations together; it has recognized that barriers between intelligence gathering and research should be broken down and has created joint intelligence spheres, allowing accessibility to every partner on a needs basis.

Generating Jointness in Intelligence: Information Systems Management Frameworks

Frameworks for managing the intelligence community help to promote jointness by means of synchronizing the various community member organizations. These organizations compete with one another for resources and prestige, often resulting in duplication and redundancy that is liable to damage their potential contribution to the community.[29] An overall supervising body could promote jointness in both the cognitive and the organizational fields. This body could operate in a top-down process to create standards, including working norms, and could oversee the establishment of shared, mission-driven frameworks that would allow several parties to work together.

The Office of the Director of National Intelligence (DNI), established in response to the commissions of inquiry in the aftermath of 9/11, manages the US intelligence community. Until then, the Central Intelligence Agency (CIA) had been in charge of the intelligence community. The new body was given the authority to formulate the intelligence policy of the United States, direct the intelligence program and its budget, make recommendations for senior appointments in the intelligence agencies, and establish joint intelligence service teams. The DNI advances programs to increase jointness among the US intelligence bodies and promotes standards to ensure synchronicity among them. For example, the DNI promoted jointness in its "500 Day Plan: Integration and Collaboration" from 2007. The plan's stated objective was to strengthen the principles of jointness within the American intelligence community in several ways.[30] The plan was written as part of implementing the American national intelligence strategy; it presents jointness and system integration as key organizational objectives and is updated every few years.[31] It defines jointness as a multiplier force that is essential to the functioning of

all realms of intelligence activity (information technology, language, analysis, assessment, and more). The plan discusses the creation of community-wide standards for disseminating information and documents, information security, and accessibility to sources, while it also proposes the construction of a shared, uniform interface for extracting and working with pieces of information.

Another principle that the DNI promotes, also mentioned in US intelligence strategy publications, is "mission-driven intelligence workforces."[32] This principle acknowledges that the mission should determine the structures by which the intelligence activity should be organized, and not allow any formal distinction between areas of expertise and organizations to foil the reorganization or the creation of an integrative, mission-driven setting. This principle stresses the need for deciding on community-wide missions as an organizing principle and as the basis for joint planning and execution, while taking optimal advantage of the resources and capabilities of each organization and reducing any obstacles based on organizational differences.

As in the United States, Israel's intelligence organizations also seek to promote jointness and break down barriers. A key step in this direction was the 2007 establishment of an operating division in the IDF's intelligence branch—a modern reincarnation of the intelligence-gathering platoon—as a result of the lessons of the Second Lebanon War. The purpose of this division is to create better lines of communication between the various intelligence systems in the IDF's Military Intelligence Directorate, as well as between intelligence in general and the various operational field echelons. The operating division is meant to serve as a kind of operational command center for all the entities in the intelligence branch. It was given the authority to direct the special operational units subordinate to the Military Intelligence Directorate, allocate intelligence-gathering resources based on changing situational assessments, and steer joint processes.[33] The lessons of the Second Lebanon War caused the division to formulate a new understanding of compartmentalization, which allows faster and better assimilation of intelligence among the fighting forces. Training is another sphere that helps to promote jointness. For example, in the late 1970s, the IDF began a senior intra-service intelligence course whose primary purpose was to encourage cooperation by bringing together the senior members of the intelligence community. In recent years, the course has been thoroughly revamped and now focuses on creating and enabling

jointness, both within the senior management and command echelons, as well as within the professional fields.[34]

The technological transformations in the cyber era have affected greatly the ecology necessary to maintain jointness among the various intelligence services. The changes that have occurred in management and information systems have provided the intelligence community with new challenges and opportunities. This is manifested by new modes of interaction and discourse among analysts and intelligence gatherers, such as the Wiki platforms, based on the Wikipedia model—an open encyclopedia in which users create and edit entries and contribute their expertise—or social media-based platforms, in which a variety of parties concerned with a certain issue can discuss and contribute their own interpretations and insights. The discourse within the intelligence social network neutralizes any obstacles that are related to the participants' organizational memberships or ranks, which usually have considerable influence in other non-networked discourses.[35] In this context, American researchers have proposed the concept of a "shared intelligence environment" that has characteristics of social media, including virtual meetings, shared writing, and working on "living" or "dynamic" documents (documents that are continually edited and updated), blogs, and so forth.[36]

Jointness Models in the Intelligence Community: American and Israeli Case Histories

Presenting the Typology

As shown by Diagram 4 below, jointness models in intelligence may be characterized by two variables: the operational environment and the conceptual core. The first variable, the operational environment, can be described by an axis where one end represents a pure intelligence-operating environment, and the other end represents a mixed or multi-entity operating environment in which intelligence is only one of the players. A purely intelligence-operating environment relies upon intelligence methodology and concepts, while compartmentalization is limited or non-existent. In contrast, a mixed operating environment, in which intelligence is one of many entities, employs various methodologies and is characterized by different organizational identities. Intelligence is then required to adapt to different, external rules, adjust itself conceptually and operationally, and adhere to the rules of compartmentalization. The second variable—the conceptual core—

can also be described by an axis whose one end represents the conceptual idea of jointness and the other—the organizational concept. The intersection of the two axes creates a matrix of four archetypes of intelligence jointness models, as follows:

a. The first archetype represents cognitive jointness, characterized by joint thinking and learning by several players from a variety of intelligence organizations and the formulation of other intelligence concepts.
b. The second archetype also deals with the framework of jointness for thinking and designing the system; in this case, however, the intelligence organizations represent only one of a group of players, while the emphasis is placed on the development of knowledge of the system as a whole.
c. The third archetype represents intra-intelligence jointness, which takes place among those who engage in research, information gathering, cyberspace, and technology. This jointness relates to the crux of intelligence work and enables intelligence to gain the most from its capabilities.
d. The fourth archetype represents jointness between intelligence and non-intelligence systems and organizations.

This essay will expand upon the latter two archetypes.

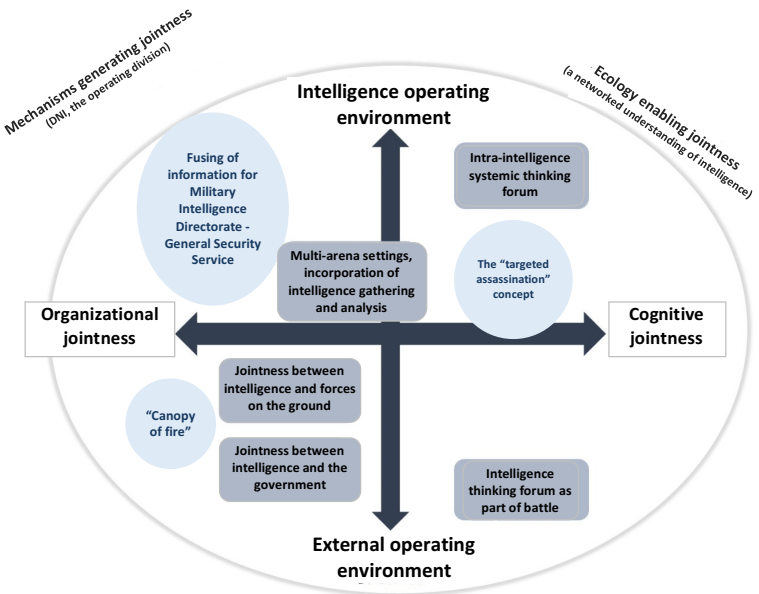

Diagram 4: Typology of Jointness Models

Examples of Jointness in Intelligence

Many examples of joint intelligence settings can be found within the American intelligence community. Well covered in the research, the National Counter Terrorism Center (NCTC) was established at the recommendation of the Commission of Inquiry on 9/11. The commission had to deal with the need for integrative intelligence assessments of various terrorist threats and for research settings that would collect the various assessments of the different entities within the American intelligence community. The NCTC represents the understanding that terrorism is a unique battlefield that integrates the internal and the external and that only an integrative intelligence community can foil terrorism, unlike the divisive nature that had characterized the US intelligence agencies until then.

The NCTC includes a large division for intelligence research, which are divided into branches corresponding to different arenas of threat. Each branch consists of representatives from several American espionage agencies.[37] The NCTC receives the raw intelligence produced by each of the espionage agencies, and its researchers must construct comprehensive, holistic assessments of the various terrorist threats. A study written by a CIA researcher,[38] who had worked for the NCTC for about two years, indicates that the NCTC's prestige and status are not on par with the other organizations whose representatives work with the NCTC; the inferior position of the NCTC is the result of the organizational and political environment in which it operates.[39] Over the years, veteran espionage organizations such as the CIA have nurtured a tradition of organizational pride that furthers intra-organizational excellence, but makes jointness with other external espionage agencies difficult.[40] As a result, employees from different espionage agencies that go to work with the NCTC tend to carefully guard their original organizational identity.

Lately, the CIA has undergone comprehensive structural change, leading to the establishment of ten geographical and topical mission centers; in each center, representatives of all the intelligence professions (covert operations, research, technology, and so forth) are active.[41] This change is an example of a new architecture of intelligence organizations, given the need for an integrative approach for dealing with the current intelligence challenges; it is not an example of inter-organization jointness, but rather of intra-organizational jointness.

Fusion Centers: Jointness Between Intelligence and Government and Civilian Sectors

Fusion centers are situation rooms that connect the activities of government and intelligence branches and serve government authorities in various states. In the United States, fusion centers operate in conjunction with the civil sector and different government departments as part of the effort to prevent terrorism, crime, and disasters.[42] In the decade after 9/11, ten fusion centers were established in the United States operating at the regional, state, and federal levels.[43] These centers are subordinate to the Department of Homeland Security (DHS) and include representatives from government agencies, the private sector, and sometimes also the military. All centers have representatives from at least one US intelligence agency, in addition to the legal system, the police and FBI, local government authorities, authorities operating national infrastructures, and the private business sector; the presence of parties from the private sector is meant to give the fusion centers access to private company data.[44] The centers receive information from a variety of sources and create integrative situational assessments, allowing them to deter, foil, warn about, and study different terrorist threats mostly at the state level.[45] By integrating data from a broad array of intelligence, legal, and government sources, the centers are able to make assessments and periodically publish documents. When there is an ongoing incident, fusion centers are responsible for supporting the operational authorities by supplying relevant information and by connecting the various authorities.[46]

The idea behind the fusion centers was to integrate the capabilities of the various government branches, based on the understanding that confronting terrorism and crime is possible only through an integrative effort. Nevertheless, in the past decade the fusion centers have come under criticism, and commissions of inquiry have been established to examine their activities.[47] The criticism has focused on the low professional level of some of the reports produced by the centers, which flooded the US intelligence community and the DHS with information about civilian activity that had nothing to do with terrorism.[48] Another problem, which was mentioned in several fusion center reports, has been the low level of trust among the team members of the various fusion centers. One of the reasons for this state of affairs is the limitation on the use of highly classified materials, which are generally revealed only to members of the intelligence community.[49]

Jointness Between Intelligence and Operational Units

Unlike the fusion centers, the intelligence-operational interface concerns operational and intelligence processes on the battlefield. This interface occurs at the stages of intelligence gathering, processing, and analysis, as well as during the operational mission itself. The presence of intelligence in or near the sphere of operations connects it to the real world and assists in producing information that is relevant to carrying out an operation and in comprehending the intelligence gathered by the forces before and during the fighting.

The American Case

In the US army, Joint Inter-Agencies Task Forces (JIATFs)[50] have been established in order to improve the ability of US intelligence and defense systems to confront armed militias and terrorist cells that are embedded in civilian surroundings. The teams are composed of representatives from several intelligence agencies and operational and administrative units who were present in areas where the US army operated; the idea of the JIATFs relates both to headquarters and field settings. The working assumption in the creation of the JIATFs is that no single agency can provide a full and reliable assessments of armed terrorist groups and cells. One of the parties of a JIATF must serve as mission leader, and this person is given the authority to manage the activity. The size of the agency represented or the scope of that agency's contribution to the mission at hand determines who leads the mission, based on the assumption that the size of the contribution or the organization's importance confers legitimacy and validity for leading the joint team.

Evidence of successful activities of JIATFs can be found in Bosnia and Iraq where jointness made it possible to identify terrorist cells and foil attacks.[51] An analysis of the activity of the teams in these regions demonstrates that the joint presence of representatives from different intelligence and army units in highly dangerous conditions far from their home bases was the key factor that removed the psychological obstacles and generated an atmosphere of openness and cooperation. The smaller the JIATFs were, the greater the intimacy that was created, and this allowed for efficient working processes and more significant outcomes.

The Israeli Test Case: Confronting Palestinian Terrorism

Since the early 2000s, Israel's military intelligence and the General Security Service (GSS; in Hebrew, known as the Shin Bet) have stood at the forefront of the battle against Palestinian terrorism. The crisis that Israel experienced in facing the suicide terrorists during the Second Intifada led to the development of highly effective intelligence and operational jointness, which since then has been used in routine times and war. During the long years of confrontation with the Palestinians, Israel's military intelligence transformed from being charged with helping in decision making to formulating strategy and shaping military campaigns and being a significant operational tool,[52] which focused primarily on "completing the circle," or retaliation as a response to terror.[53]

The concept that prevailed within the Israeli intelligence community in the 1990s for regulating relations between the Military Intelligence Directorate and the GSS was the "Magna Carta." To a great extent, one can view the "Magna Carta" as the reverse of the jointness approach, because it drew clear lines of responsibility between the intelligence services and defined spheres of activity and authority, leaving almost no room for joint action. After a few years of fighting terrorism together, in a period described as "years of mass arrests and targeted assassinations," the institutions of the intelligence community, especially the Military Intelligence Directorate and the GSS, grew closer to one another;[54] an atmosphere of trust and intimacy ensued, quite distinct from the atmosphere of disagreement that had characterized their earlier relationship.

Yuval Diskin, then deputy head of the GSS, pioneered the concept of "joint prevention conception," the purpose of which was to maximize intelligence and operational capabilities in order to engage in targeted killings. Under his leadership, the GSS did away with the compartmentalization that had separated the organization's geographical units because terrorist organizations crossed geographical borders and therefore a more comprehensive approach to the entire Palestinian system was necessary. Diskin also promoted channels of dialogue and coordination with Unit 8200 of the Intelligence Corps, which is responsible for collecting signals intelligence (SIGINT), and integrated its representatives in the GSS's geographical control rooms so that SIGINT could be employed for operational closure. He acted similarly with IDF operational units in the West Bank and Gaza Strip and with the Israeli Air Force.

Removing the barriers that were created by compartmentalization and creating a joint presence in command and control rooms not only led to an atmosphere of trust and openness, but also to a common language that helped to develop and forge a consciousness of jointness in the different organizations. The joining of forces within the internal environment of the intelligence agencies and in the external environment between intelligence organizations and operational units made it possible to achieve new operational goals. At a later stage, the Military Intelligence Directorate and the GSS succeeded in developing jointness at a very high level, based on fusing information from among all the intelligence gathering and research agencies. The last three rounds of fighting in the Gaza Strip (2009, 2012, and 2014) were good examples of inter-organizational jointness, which enabled information to be shared so that a high level, large "bank of targets" could be created.[55] Another expression of jointness between intelligence bodies and operational-fighting units is the "canopy of fire" project—the IDF's version of the targeted assassination model developed by the GSS. In the context of that project, parties in both intelligence and the Israeli Artillery Corps or the Air Force operate in joint attack units to foil rocket launching and anti-tank cells and to thwart the penetration of terrorists into Israel.[56]

Conclusions and Insights

The recent decades have witnessed significant changes in the concept of jointness and its practical application. At the beginning of the twenty-first century, jointness became an important tool of intelligence communities, as a result of changes to the security environment in which they operate, the intelligence challenges and the subsequent crises that affected them, in addition to the technological and cultural transformations.

Jointness describes a complex, multi-dimensional interface between entities; at its core are processes of learning at different levels, which are facilitated by a particular organizational ecology. The understanding that many working environments can be more relevant and effective thanks to the interface of jointness is not intuitive; furthermore, jointness is possible only when organizations concede some of their authority and share responsibility with others. The challenges that the organizations faced and the crises that hit them as a result revealed gaps in their relevance, which in turn, generated a willingness to engage in jointness.

This essay surveyed the theoretical and practical development of the jointness approach, distinguished between cognitive jointness and organizational jointness, and examined the interrelations and connections between them and the types of learning. The matrix created by the intersection of the axes of the two variables (the operational environment and the conceptual core) makes it possible to identify and define four archetypes or models of jointness, which the essay analyzed, using several cases studies from both the United States and Israel.

Jointness is not a magical solution; it has not proven to be the best organizational solution in every situation in which it has been tried. Test cases also show that jointness is not always properly applied. Its success depends on several components, which, when viewed together, can be referred to as the organizational ecology. The most prominent component is organizational freedom, and creating a space in which it is possible and even recommended to give autonomy to the various players. This autonomy allows for flexibility and creativity, even if it means straying from familiar working methods. Furthermore, trust among the players is very important for the success of the interfaces. Jointness among various members of a single intelligence community, and, in particular, jointness between intelligence agencies and external parties, is possible mainly in situations in which intelligence personnel are able to develop expectations of positive behavior from their partners and reduce their concerns about negative behavior. This builds trust, which increases players' willingness to take chances, including revealing themselves and sharing with each other. The notion of an overarching body (such as the DNI in the United States) that facilitates and generates jointness and can influence the organizational ecology has emerged as important, at least in the context of the American intelligence community. A director of such a body can encourage the creation of a conducive climate for jointness, as well as promote awareness and the values needed for engaging in shared work.

The ultimate manifestation of intelligence jointness is in the multi-arena setting that incorporates intelligence gathering and research bodies. This model represents aspects of both cognitive and organizational jointness, from processes of thinking and learning in its making to the way in which it is realized. In these cases, jointness indicates an understanding that the format of traditional intelligence work that is split among various disciplines needs to be changed to mission- or arena-driven intelligence production.

In conclusion, jointness is a response to some of the key issues that the intelligence communities are currently confronting; adopting the concept of jointness would enable them to provide a better solution to these challenges. At the same time, it is not a panacea that obviates the need for traditional concepts and organizational structures. Realizing jointness in places and contexts where it is needed also requires shared force construction, such as personnel, communications infrastructures, and more, all which form a critical foundation for attaining this objective.

Notes

1 The first seeds of jointness can be traced to Soviet military thought on the art of the campaign. For more on this topic, see Shimon Naveh, *The Art of the Campaign: The Making of Military Excellence* (Tel Aviv: Ministry of Defense Publications and Maarakhot, 2001) (Hebrew).

2 US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC, amended through September 17, 2006), p. 132.

3 An example is the US naval strategy, "Ship Maritime Strategy 600," which involved warships and aroused the ire of the heads of the other branches when it was presented. See Don M. Snider, "The US Military in Transition to Jointness Surmounting Old Notions of Interservice Rivalry," *Airpower Journal* 10, no. 3 (Fall 1996), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/fall96/snider.html.

4 Ibid.

5 The text of the act is available at "Goldwater-Nichols Act of 1986," US Code Legal Information Institute, Cornell Law School, http://www.au.af.mil/au/awc/awcgate/congress/title_10.htm; for more on the act, see "Goldwater-Nichols Act," Wikipedia, https://en.wikipedia.org/wiki/Goldwater%E2%80%93Nichols_Act.

6 Joint Chiefs of Staff, *Joint Warfare of the US Armed Forces*, Joint Publication 1 (Washington, DC: National Defense University Press, November 11, 1991), http://hdl.handle.net/2027/uiug.30112001695292.

7 The doctrine was shaped hierarchically in a top-down manner, unlike the navy doctrine, which was formulated by the different fleets in a bottom-up fashion. For more, see Paul J. Bolt, Damon V. Coletta, and Collins G. Shackelford, *Defense Organization: The Need for Change: Staff Report to the Committee on Armed Services* (Washington DC: US Government Printing Office, 1985), http://babel.hathitrust.org/cgi/pt?id=mdp.39015011556266;view=1up;seq=1.

8 Snider, "The US Military in Transition."

9 Efron Razi and Pinhas Yehezkeli, *Public Management at a Crossroads: From Selfishness to Cooperation* (n.p.: Center for Strategy and Policy Study, National Security College, IDF, May 2007), p. 31 (Hebrew).

10 This approach to developing an application is called service-oriented architecture (SOA). See "Service Oriented Architecture (SOA) and Specialized Messaging Patterns," Adobe, 2005, http://xml.coverpages.org/SOA-Adobe20050221.pdf.
11 Zvi Lanir, "Why We Need the Concept of Jointness" *Maarakhot*, no. 401 (June 2005), p. 20 (Hebrew).
12 For more on the distinction between coordination, cooperation, and jointness, see the jointness chart at https://doalogue.co.il/wiki/.
13 Lanir, "Why We Need the Concept of Jointness," p. 25.
14 Razi and Yehezkeli, *Public Management at a Crossroads: From Selfishness to Cooperation*, p. 59.
15 Ibid, p. 53.
16 US Department of Defense defines "Jointness of the Joint Force" as follows: "Jointness implies cross-service combination wherein the capability of the joint force is understood to be synergistic, with the sum greater than its parts (the capability of individual components)." It defines "Joint Operation Planning" as providing "a common basis for discussion, understanding, and change for the joint force, its subordinate and higher headquarters, the joint planning and execution community, and the national leadership." See United States Department of Defense, *Doctrine for the Armed Forces of the United States* Joint Publication 1 (Washington DC: United States Department of Defense, March 2013), pp. xii, ix, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.
17 US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, pp. 11, 13–14.
18 Doctrine Department, Safety and Training Commands, "Lexicon (2006)," in *Systemic Planning* (IDF, Operations Division, Doctrine Training), (Hebrew).
19 For more on the distinction between forming and planning in the system's jargon, see Yotam Hacohen, "Forming the Campaign," Doalogue, (Hebrew), https://doalogue.co.il/wiki/עיצוב המערכה.
20 Kobi Michael, "The Failure of Learning in the Test of Matching Statesmanship to Militarism in the War on Terrorism in the Middle East," *POLITIKA—The Israeli Journal of Political Science and International Relations* 25 (2015): 6 (Hebrew).
21 Gabriella Heichal, *Decision Making in a Crisis* (Tel Aviv: Maarakhot, 1992), pp. 75–79 (Hebrew).
22 Kobi Michael, "Who Really Dictates What an Existential Threat Is? The Israeli Experience," *Journal of Strategic Studies* 32 no. 5 (2009): 687–713.
23 Roy J. Lewicki, Daniel J. McAllister, and Robert J. Bies, "Trust and Distrust: New Relationships and Realities," *Academy of Management Review* 23, no. 3 (July 1998): 438–458.
24 This model was presented by Daniel Bar-Tal at a research workshop held at the Tami Steinmetz Center for Peace Research at Tel Aviv University.
25 Jeanne Hull, "'We're All Smarter than Anyone of Us': The Role of Inter-Agency Organizations in Combating Armed Groups," *Journal of International and Public Affairs* (2008): 37–38.

26 Itai Brun, *Intelligence Research: Clarifying Reality in an Era of Change* (n.p.: Israel Intelligence Heritage and Commemoration Center (IICC), The Institute for Intelligence and Policy Research, Effi Meltzer Ltd., 2015), p. 97 (Hebrew).
27 For more on the challenge in surveilling a disappearing enemy, see ibid, p. 93. On the challenge in the making, see ibid, p. 32.
28 Ibid, p. 12.
29 Bridget Rose Nolan, "Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center," (PhD diss., University of Pennsylvania, 2013), p. 158.
30 United States, Office of the Director of National Intelligence, *500 Day Plan, Integration and Collaboration* (October 10, 2007), http://fas.org/irp/dni/500-day-plan.pdf.
31 United States, Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America* (September 2014), http://www.odni.gov/files/documents/2014_NIS_Publication.pdf. The idea was referred to in several versions of the document over the years between 2005–2014. For 2005, see http://fas.org/irp/offdocs/nis.pdf; for 2009, see http://fas.org/irp/offdocs/nis2009.pdf. See also Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0 (October 2013), http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.
32 See, for example, United States, Office of the Director of the National Intelligence, *The National Intelligence Strategy of the United States of America* (August 2009), p. 11.
33 Amir Rapaport, "Upheaval in Intelligence," Israeldefense, March 6, 2014 (Hebrew), http://www.israeldefense.co.il/he/content/טלטלה-מודיעינית.
34 Shai Shabtai and Omri Gefen, *Promoting Jointness in the Intelligence Community Using the Senior Inter-Service Intelligence Course* (internal publication, 2015), (Hebrew). The document was presented to an intelligence forum at the Institute for National Security Studies.
35 David Siman-Tov and Ofer G., "Intelligence 2.0: A New Approach to Intelligence Production," *Military and Strategic Affairs* 5, no. 3 (December 2013): 31–51, http://www.inss.org.il/uploadImages/systemFiles/MASA%20-%205.3.pdf.
36 Chris Rasmussen, "Toward Living Intelligence," Gov 2.0 Expo Showcase, Washington DC., September 8, 2009, http://www.gov2expo.com/ gov2expo2009/public/schedule/detail/10599. See also the YouTube video at http://www.youtube.com/watch?v=XdQPuTVDOH4.
37 These include the National Geospatial-Intelligence Agency (NGA), Federal Bureau of Investigations (FBI), Defense Intelligence Agency (DIA), National Security Agency (NSA), and the CIA.
38 Nolan, "Information Sharing and Collaboration in the United States Intelligence Community."
39 Ibid, p. 59.
40 Ibid, p. 70.

41 Tom Ashbrook, "Reforming the American Intelligence System," On Point Radio Show, March 11, 2015, http://onpoint.wbur.org/2015/03/11/cia-reform-john-brennan-senate-spies-national-security.
42 Gudrun Persson, *Fusion Centers—Lessons Learned—A Study of Coordination Functions for Intelligence and Security Services* (Swedish National Defense College, 2013).
43 The list of fusion centers active in the United States may be found at the official website of the DHS, at Fusion Center Locations and Contact Information, http://www.dhs.gov/fusion-center-locations-and-contact-information.
44 Torin Monahan, "The Murky World of Fusion Centers," *Criminal Justice Matters* 75, no. 1 (2009): 20–21, http://publicsurveillance.com/papers/FC-CJM.pdf.
45 US Department of Homeland Security, US Department of Justice, Fusion Process, Technical Assistance Program and Services, *Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness*, *Comprehensive Preparedness Guide (CPG) 502* (May 2010), p. 9, https://www.fema.gov/media-library-data/20130726-1828-25045-3917/cpg_502_comprehensive_preparedness_guide_considerations_for_fusion_center___eoc_coordination_2010.pdf.
46 Chuck Dodson, "Use of Technology in Intelligence Fusion Centers," An Oracle White Paper, April 2007, p. 5, http://www.oracle.com/us/industries/046140.pdf.
47 For the report of a federal commission of inquiry to examine the activity of the fusion centers, see US Senate, The Permanent Subcommittee on Investigations, "Investigative Report Criticizes Counterterrorism Reporting, Waste at State & Local Intelligence Fusion Centers," Press Release, October 3, 2012, http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.
48 For an essay describing the damage to privacy generated by the fusion centers, see Robert O'Harrow, "DHS 'Fusion Centers' Portrayed as Pools of Ineptitude and Civil Liberties Intrusions," *Washington Post*, October 2, 2012, http://www.washingtonpost.com/investigations/dhs-fusion-centers-portrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cb1-11e2-bd1a-b868e65d57eb_story.html.
49 Persson, *Fusion Centers—Lessons Learned*, p. 12.
50 Hull, "We're All Smarter than Anyone of Us."
51 Ibid, p. 37.
52 Lt. Col. A., "The Place for Intelligence in the Clausewitz Triangle," *Maarakhot*, no. 409–410 (December 2006): 77–81 (Hebrew).
53 Amir Oren, "The master of interpretations or the servant of operations," *Haaretz*, June 24, 2005 (Hebrew).
54 Ibid.
55 In reference to Operation Cast Lead, see Yossi Melman, "The wonders of fusion," *Haaretz*, August 1, 2008 (Hebrew).
56 Amir Bohbot, "Intel gathering officer: The story of a targeted assassination," *Walla*, December 28, 2012, http://news.walla.co.il/item/2601434 (Hebrew).

The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking

Omry Haizler

This article will touch upon two main components of the United States' cybersphere and cyber warfare. First, it will review three cyber incidents during different time periods, as the US infrastructure, mechanisms, and policies were gradually evolving. It will analyze the conceptual, operational, and legislative evolution that led to the current decision-making paradigm and institutional structure of the US cybersphere. Secondly, the paper will examine the procedures and policies of the Intelligence Community (IC), and the US cyber operational structure. It will review the missions and background of the IC and its responsibilities before, during, and after a cyberattack, and will touch upon the IC's organizational architecture. The paper will also briefly review the current cyber threats in the United States and will elaborate on some of the fundamental strategies and policies that it uses to provide a suitable response. Lastly, it analyzes the cybersphere's macro-level, addressing the data coordination of the IC's agencies, as well as the federal, state, and private sector institutions during a cyber crisis.

Keywords: Moonlight Maze, Morris Worm, Stuxnet, cyberattacks, United States intelligence community, cyber crisis, cyber threats, internet governance, cyber policy, cyber strategy

Omry Haizler is a former IDF Officer and a Prime Minister's Office operative. He holds an MPA from Columbia University's School of International and Public Affairs (SIPA). He currently teaches at Columbia's School of Continuing Education.

History of Cyber Warfare

There are three historical stages of the evolution of cyber warfare: 1) the realization phase during the early era of the internet; 2) the takeoff phase during the interim period of pre- and post- 9/11 in which attacks were still mainly of an information-gathering nature; and 3) the modern militarization phase, during which cyber warfare may cause similar damage to US strategic capabilities and critical infrastructure as a kinetic attack on a colossal level. Figure 1 below describes these stages:[1]

Stages	Realization	Takeoff	Militarization
Timeframe	1980	1998–2003	2003–present
Dynamics	Attackers have advantage over defenders	Attackers have advantage over defenders	Attackers have advantage over defenders
Who Has Capabilities?	United States and few other superpowers	United States and Russia with many small actors	United States, Russia, China, and many more actors with substantial capabilities
Adversaries	Hackers	Hacktivists, patriot hackers, viruses, and worms	Neo-Hacktivists, espionage agents, malware, national militaries, spies, and their proxies, hacktivists
Major Incidents	Cuckoos Egg (1986), Morris Worm (1988), Dutch Hackers (1991), Rome Labs (1994), Citibank (1994)	Eligible Receiver, Solar Sunrise, Moonlight Maze, Allied Force, Chinese Patriot Hackers	Titan Rain, Estonia, Georgia, Buckshot Yankee Stuxnet
US Doctrine	Information warfare	Information operations	Cyber warfare

Figure 1: Phases of Cyber Conflict History

Attacks as Catalyzers for Institutional Evolution

Each of the above periods characterizes a fundamentally different doctrine, both with respect to technological progression and type of threats, and to the administration's cyber policies at each given time. Certain past attacks embodied future cyber challenges, serving as warning signs to institutions' vulnerabilities and lack of security. As society's dependency on technology

increased, the possible ramifications of inefficient security in a specific breach also increased.

1. Realization—the Morris Worm

This cyber incident acted as the first wake-up call to the American Intelligence Community (IC), policymakers, and academics. While it was not the first cyberattack on US computer systems—the 1986 Cuckoo's Egg hack involving the Soviet KGB was the first significant cyber espionage attack—it is widely considered the first large-scale attack, both in terms of the quick phase of events, its scale, and its implications. Launched as a prank from a lab at Cornell University, the Morris Worm was designed to infect as many machines as possible without being detected; the worm crashed 6000 computers—roughly 10 percent of the internet in 1988.[2] The US Government Accountability Office assessed the damage at $100,000–$10,000,000, illustrating the difficulty of assessing cyberattack damage, a problem prevalent even today.[3] Despite the severe ramifications, the incident provided an important warning to the IC, highlighting the potential dangers of highly connected computer networks and the need for institutionalized defensible capabilities and structures in the cybersphere.

The Morris Worm acted as a catalyzer for the first steps towards a more regulated cyberspace and led to dramatic changes, both conceptually and operationally:

Paradigm Shift: At the time of the incident, the internet was taking its first substantial steps and was considered a "friendly place," where everyone knows everyone. The Morris Worm made it clear that some people in cyberspace did not have the best interests in mind; the incident was the first time where cyber innovation shifted from focusing solely on interconnectivity to security concerns.

Operations: Established after the Morris Worm incident by the Defense Advanced Research Projects Agency (DARPA) at Carnegie Mellon University, the Computer Emergency Response Team (CERT) demonstrated the shift from ad hoc solutions to professional teams, which were trained and equipped to coordinate events and provide assessments and solutions to a given cyberattack.[4]

Regulations: Along with the conceptual shift in cybersecurity, Congress passed several laws in the years following the Morris Worm incident, including

the Electronic Communications Privacy Act of 1986 and the Computer Security Act of 1987 to ensure privacy in cyber domains through legal protections.[5] Additionally, Robert Tappan Morris who created the Morris Worm, was the first person to be convicted under the new Computer Fraud and Abuse Act of 1986.[6]

2. Takeoff—The Moonlight Maze

In 1998, US officials accidentally discovered a pattern of sustained probing of the Pentagon's computer systems, private universities, NASA, Energy Department, and research labs. Soon they learned that the probing had occurred continually for nearly two years. Thousands of unclassified, yet sensitive documents relating to technologies with military applications had been examined or stolen, including maps of military installations, troop configurations, and military hardware designs.[7] Although the Defense Department traced the trail back to a mainframe computer in the former Soviet Union, the sponsor of the attacks remains unknown. Russia denied any involvement, and the suspicions have never been conclusively proven.[8]

Moonlight Maze is widely considered the first large-scale cyberespionage attack by a well-funded and well-organized state actor. The attack was well planned as the attackers left "backdoors" to enable hackers to penetrate the system at different times, left few traces, and continued for a long time without detection.[9] Moonlight Maze highlighted the increasing role of state authorities in generating, sponsoring, or, at least, passively tolerating sophisticated and far-reaching espionage incidents. Moreover, it stressed the vulnerabilities of the infosphere, in which adversaries could not only cause disruption of service, but also could exploit sensitive information. It emphasized the crucial need for firewalls and encryptions and, above all, the difficulties of identifying and attributing an attack to a specific adversary. Moonlight Maze was an important progression in cyber warfare and cybersecurity due to its implications on future conflicts.[10] It pointed out the future shift in the modern battlefield from a kinetic war—in which enemies have names and physical locations, and in which attacks can be witnessed and assessed—into an asymmetrical warfare with offensive cyber operations, where attacks might be invisible, adversaries are unknown, and damage is hard to quantify. The incident led to dramatic shifts in the US administration's approach to cybersecurity.

Paradigm Shift: The awareness of terrorist threats and support of counterterrorism initiatives post 9/11 among policymakers were limited. The Moonlight Maze incident caused a rethinking of the US cyber defense strategy, cyber warfare attribution, cyber deterrence, and the current defense of sensitive, non-encrypted networks such as NIPERnet (Non-Secure Internet Protocol Router Network, the Pentagon's non-classified network). For the first time, political and constitutional questions were raised about security, privacy and notions of active monitoring and possible exposure to transnational threats.[11] Moonlight Maze caused the US agencies and government to realize that clear policies and strategies were needed for asymmetric warfare, the field of future intelligence gathering and espionage, and the technological implications they entail.

Legislative Acts: The Presidential Decision Directive 63 (PDD 63), regarding critical infrastructure protection, was, in part, the result of Moonlight Maze. This was a seminal policy document setting forth roles, responsibilities, and objectives for protecting the nation's utility, transportation, financial, and other essential infrastructure.[12] The PDD 63 led to two significant strategic implications. One was the creation of the National Incident Protection Center (NIPC), an inter-agency body with the power to safeguard the nation's civilian and governmental critical infrastructure from computer-based attacks.[13] The second was the creation of the Joint Task Force Computer Network Defense (JTF-CND), a body entrusted with taking the lead in coordinating a response to national cyberattacks and centralizing the defense of military networks.[14]

Operational: Led by the Department of Defense (DoD), incident response mechanisms were built and reporting institutions were established. Military reports would be handled at the local level through Network Operations and Security Centers (NOSCs) under the Defense Information Systems Agency (DISA). Handled as command and control mechanisms, regional CERTs are at the frontline of assessing impact on an individual and regional level. JTF-Computer Network Operations (CNO) and the DISA Global Network Operations and Security Center (GNOSC) are additional factors that expedite channeling of information.

3. Militarization—Stuxnet

The Stuxnet attack is considered one of the most sophisticated malware attacks publicly recorded. Although unverified, many experts argue that only

a nation-state could have created and launched the attack and many media outlets suggested it was a joint Israeli-American operation.[15] Considered as one most impactful cyberattacks involving sovereign countries, the malware damaged Iran's centrifuges and delayed its uranium enrichment efforts. Once inside the network, it used a variety of mechanisms to propagate to other machines within that network and gain privileges as soon as it had infected those machines. These mechanisms included both known and patched vulnerabilities, as well as four vulnerabilities that were unknown and unpatched when the worm was released (aka "zero-day" exploits).[16] While the international community remains unsure of the source and exact purpose of the virus, the incident raised awareness of networks' vulnerabilities.[17]

Identified in 2010, Stuxnet's impact and unclear origin highlight the difficulty in noticing an attack and suggest that at a nation level, it is impossible to fully defend all vital resources.[18] Therefore, it became crucial to understand the dynamics of battle-like situations in modern-age cyber warfare, in which even a colossal attack does not necessarily have an attributed attacker or a trace of any attack at all. This means that in modern non-kinetic battle fields, policymakers realize the effect of an attack (from denial of service to the destruction of a nation's critical infrastructures) without having a smoking gun or any legal or political tool to fight with. This phenomenon requires legislators and authorities to start formulating response options and detailed protocols now, rather than trying to develop ad hoc options later during a crisis.

The cyber warfare of post-2013 shifted the counterattack approach from an operational level[19] to a strategic-diplomatic one, where policy, international laws, internet governance, and agreements play a significant part in the overly-breached cyber environment. Three substantial internet governance agreements and collaborative efforts have taken place on a multinational level:

a. The United States-China Cyber Agreement: This agreement ensures that neither government "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."[20] While it is only a basic agreement that does not ensure a safe cyber environment between the two states, its importance stems from the ability to build upon it in future years and act as a gesture of goodwill.

b. The United Nations' World Summit on the Information Society process (WSIS+10): This summit renewed the Internet Governance Forum (IGF), a venue where member states, civil society, and the private sector debate internet policy, cybersecurity, surveillance, intellectual property, and copyright. Nations have strengthened diplomatic, open channels regarding cyber policy, reiterating their commitment to bridge the digital divide and improve access to information and communications technologies (ICTs), by recognizing the WSIS+10 document.[21]
c. The Safe Harbor Agreement: This agreement was signed between the US Department of Commerce and the European Union and regulates the way that US companies can export and handle the personal data of European citizens for the first time.[22]

US Cybersphere Operational Structure

Due to the complexity of coordination, fragmented responsibilities, and overlapping oversight, the multi-faceted cyberspace is saturated with military, think tanks, academia, private sector and government institutions, branches, and offices. At the national level is the Intelligence Community, which has both defensive and offensive capabilities and has the ultimate responsibility in addressing and monitoring modern cyber warfare. Whether it is an attack against military or government offices, or a significant attack against a private institution or critical infrastructure, the IC holds the operational responsibility for all aspects of the United States' cybersphere.

Established in 1981, the IC is a federation of seventeen US government agencies that work separately and together to conduct intelligence activities.[23] Member organizations include intelligence agencies, military intelligence, civilian intelligence, and analysis offices within federal executive departments, all headed by the director of National Intelligence who reports directly to the president.[24] While most of the associated agencies are offices or bureaus within federal executive departments, nine of them operate under the Department of Defense, and together spend 85 percent of the total US intelligence funds.

Traditional intelligence gathering relies on a counterterrorism's intelligence cycle, which includes human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT). While all disciplines are still needed to form an inclusive intelligence assessment, cyber and cryptology capabilities have

gained more recognition as the need for investment in human capital and resources rises and as the world's reliance on technology increases.

The IC focuses on three aspects of maintaining cybersecurity: organization, detection, and deterrence. Various organizations within the IC pursue different tasks.[25] The Office of the Director of National Intelligence (ODNI) heads a task force coordinating efforts to identify sources of future cyberattacks. The Department of Homeland Security (DHS) leads the protection of government computer systems. The DoD devises strategies for potential cyber counterattacks. The National Security Agency (NSA) monitors, detects, reports, and responds to cyber threats. The Federal Bureau of Investigation (FBI) leads national efforts to investigate and prosecute cybercrimes. Many other cyber organizations outside the IC's umbrella address cyber threats, the most prominent of which is the US Cyber Command (USCYBERCOM). During a crisis, the IC assesses intelligence within its seventeen agencies, and then formulates overall intelligence recommendations by the ODNI.

In 2015, James Clapper, the director of National Intelligence who oversees the IC and is responsible for the complex coordination between all the arms of the IC, released a risk-assessment in which cyber threats top the list of global threats,[26] ahead of physical terrorism for the first time since the attacks of September 11, 2001. Although cyberattacks against the United States are constant and on the rise,[27] Clapper referred to the possibility of a "cyber Armageddon" (aka "cyber Pearl Harbor," or "cyber 9/11") [28] as currently remote. Rather than a "cyber Armageddon" scenario that debilitates the entire US infrastructure, the IC predicts a different challenge. It foresees an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.[29] The global proliferation of malicious code increases the risk to American networks, sensitive infrastructure, and data. While a disruptive or destructive cyber operation against a private corporation, an industrial control system, or a defense system requires a potential adversary to have a significant level of expertise to execute it, it does not necessitate state-level financial abilities or world-class operational talent. A given actor, whether a nation-state or a non-state group, can purchase malware, spyware, zero-days, and other capabilities on the black market, and can pay experts to search for vulnerabilities and develop exploits. In a global environment brimming with adversaries, as well as a lack of international cyber laws and

clear regulations, these threats have created a dangerous and uncontrolled market, which serves multiple actors within the international system.[30]

Despite the increase in cyber activity by non-state actors, top US intelligence officials still believe that state actors are the greatest threat in cyberspace to US interests. The IC identifies several potential actors who may cause a cyber crisis, including nation-states with highly sophisticated cyber programs, such as Russia or China;[31] nations with lesser technical capabilities, but possibly more disruptive intent, such as Iran or North Korea; non-state actors with accessibility to significant resources and motivation to create cyber chaos; and profit-motivated criminals and ideologically-motivated hackers or extremists.

The various possible targets include:

a. The Private sector: This sector is identified not only as a victim of cyberattacks, but also as a participant in investigations and attribution. Given the importance of financial institutions (e.g., Goldman Sachs) to the economy in their dependency on technology, this sector is an important field to defend in case of a serious attack.[32]
b. Critical infrastructure: The critical infrastructure—the physical and virtual assets, systems, and networks vital to national and economic security, health, and safety—is vulnerable to cyberattacks by foreign governments, criminal entities, and lone actors. A large-scale attack could temporarily halt the supply of water, electricity, and gas; hinder transportation and communications; and cripple financial institutions.[33]
c. Government: Penetrating the US national decision-making apparatus and Intelligence Community will remain primary objectives for foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US research institutions dealing with defense, energy, finance, dual-use technology, and other areas will be a persistent threat to US interests.[34]
d. Military and government agencies: These are the front line of both defense and offense, as its infrastructure must defend the entire nation as well as its own resources in case of a full-scale cyber conflict. IC assumes that in a cyber crisis, this "contact-line" will be attacked and damaged.

The Intelligence Community Policies

The IC conducts a variety of intelligence operations on a daily basis. The United States is under constant cyberattack from both state and non-state

actors. On the national intelligence level, being under cyberattack means not only a defensive effort, but also designing various operational options for retaliation. Given its size, the IC interacts and collaborates with agencies on the operational level (military, DoD, DHS) and the state and federal level (private sector on a large scale, Department of State, White House).

The IC's strategic preparation goals[35] include:

a. Building and maintaining ready forces and capabilities to conduct cyberspace operations;
b. Defending its own information network, securing data, and mitigating risks to missions;
c. Preparing to defend US homeland and US vital interests against disruptive or destructive cyberattacks of significant consequence;
d. Building and maintaining viable cyber options and planning to use those options to control conflict escalation and to actively extract information to prepare "target banks";
e. Building and maintaining robust international alliances and partnerships to deter shared threats and increase international security and stability.

IC's policy of cyberattack response is as follows:

a. Identifying attacks: As part of the modern cyber battlefield, sophisticated attackers will attempt to conceal the attack. Just as in a conventional conflict, intelligence is needed to prepare the battle ground and accurately assess the probability of success and utility for any kind of operation.[36]
b. Informing: Although the IC has significant offensive abilities, its main role is to assess, inform, and report. The IC must inform the operational arms it collaborates with and the State Department. That is, under attack, the IC's success is measured by the precautions it gave prior to the attack and by its responsiveness, communication, and guidance during the attack.
c. Providing options: The IC must provide a set of options to decision makers and enable strategic flexibility by providing valuable information. The IC administers guidance during attack and provides strategic-operational and political leeway with its recommendations and intelligence assessment.
d. Damage Assessment: Unlike the conventional battlefield, a cyberattack may be hard to detect at times, even if it is a large-scale attack. The IC must assess the damage caused so that it can provide policymakers with the ability to retaliate in a measurable manner. This does not necessarily require operational efforts during an attack, but rather assessment,

coordination, and information-sharing with other offices so that there is an efficient flow of information.

Multidimensional Cyber Response

The IC's role overlaps in many ways with different institutions, governmental departments, and military units, many of which is out of its jurisdiction. While it does not singularly have responsibility for cyber response at the national or state level, the IC demands a complex chain of information flow and hierarchy. Other institutions that provide cyber responses are:

a. Department of Homeland Security: As part of its role to protect the United States' territories and respond to terrorist attacks, man-made accidents, and natural disasters, the DHS is in charge of Coast Guard Intelligence (CGI) and the Office of Intelligence and Analysis (I&A). The latter is responsible for managing the collection, analysis, and fusion of intelligence. The Office of I&A disseminates intelligence throughout the DHS and to the other members of the IC community, and is the first responder at the state, local, and tribal levels.[37] The ODNI is responsible for an efficient information flow between the rest of the intelligence community and the DHS in order to create synergy of information during a cyberattack.
b. Department of Defense (DoD): Considered the focal point for the intelligence community's operational source and leading nine of its agencies, including the NSA, the DoD is the ODNI's main source of cyber intelligence. As such, the Director of National Intelligence (DNI) often reports to decision makers and the White House based on the intelligence received from the DoD. In addition, the NSA and CYBERCOM, led by Admiral Michael Rogers, and the DNI, work closely together during an attack. It is necessary that the operational data stream be processed through the ODNI and received as policy recommendations at the federal level.
c. State Department: The government is dependent on the IC during a cyber crisis. Unlike in conventional conflicts, it is safe to assume that decision makers often do not know what has happened and do not know the origin of an attack in a cyber crisis scenario. It is up to the IC to provide an intelligence assessment in a timely manner and to pass on the data. Small centers that are trusted to evaluate and coordinate serve as liaisons between state institutions and the cyber intelligence field, such as the National Cybersecurity and Communications Integration Center

(NCCIC), the United States Computer Emergency Readiness Team (US-CERT), and the Cyber Threat Intelligence Integration Center (CTIIC). Stationed in the Office of the Director of National Intelligence, the latter will mirror the efforts and assessments for counterterrorism information sharing during cyberattacks.[38]

d. Private Sector: Infrastructure cyber breaches and attacks have been defined as the number one threat of the United States in 2015 by the DNI. The Information Sharing and Analysis Center (ISAC) is the main actor in overseeing private sector cyber threats, as ISAC assists federal and local governments with information pertaining to cyber threats. Private sector cyber crises may affect national interests (e.g., the Sony incident), and thus, in collaboration with DHS, Department of State, and the FBI, the private sector demands that an operational intelligence approach be taken at the national level.

Conclusions

The history of cyber warfare poses many lessons, and may indicate the progression and direction of the cybersphere, as well as the comprehensive attention required by the field at all levels. Cyber warfare's natural evolution is an important tool to assess mistakes and project the future of the infosphere, privacy regulations, cyber espionage, and cybersecurity needs. Policymakers are addressing the cybersphere today more seriously than ever before, and institutions at all levels are directing substantial resources to address cyber threats. Intelligence agencies constantly are perfecting their defensive and offensive cyber capabilities. Private institutions, especially in the fields of medicine, finance, critical infrastructure, and energy, in addition to data-driven corporations, allocate more resources and human power to data protection and cybersecurity than ever before. Lastly, the American government is aware of the risks to its own networks, and while breaches are more common than ever, investments to nurture a more defensible cyber space are at an all-time peak.

There are several fundamental policy realizations at the international level. Most policymakers and legislators do not have a comprehensive capacity to address international cyberattacks. For example, there is not an all-inclusive definition for "acts of war" in the non-kinetic sphere, and the existing definitions are unclear and not shared and agreed upon at the international

level. Moreover, retaliation mechanisms for a financial cyber crisis are not in place, preventing nation-states from attributing large-scale attacks to specific attackers and allowing other actors to avoid accountability. International collaboration at all levels, especially in the financial, diplomatic, and the judiciary fronts, are in need, as a lack of collaboration may prevent a stable foundation upon which accountability mechanisms can be formed. Despite the growing multisector investments in cybersecurity, more sophisticated attacks have taken place in the last three years than previously. Therefore, it appears that only multinational, substantial, and binding cyber agreements and progressive internet governance legislation will allow for a substantially safer cybersphere.

On the security front, the IC forms narrative and operational recommendations to policymakers, due to its coordination ability and vast jurisdiction. The biggest challenge during a cyberattack is to identify and connect the different dots for generating a responsible and measurable response. Without a body like the IC, the abundance of data would get lost in a maze of information. Just like in a kinetic battlefield, the defense line will eventually be penetrated, given a persistent attacker. Unlike the classic battlefield, however, a given cyberattack may not be seen, attribution may not be plausible, and the impact may not be noticeable. Cyber terrorism may become a growing concern with time and may require greater international intelligence collaborations than ever. Internal national intelligence security agencies may be forced to change disciplines and shift their strategic attention. It is thus plausible to project that in the future, nuclear weapons will no longer be the ultimate and greatest threat.

Notes

1 Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

2 Ted Eisenberg et al., "The Cornell Commission: On Morris and the Worm," *Communications of the ACM* 32, no. 6 (1989): 706–709, http://portal.acm.org/citation.cfm?id=63526.63530.

3 During the Morris appeal process, the US Court of Appeals estimated the cost of removing the virus from each installation was in the range of $200–$53,000. Possibly based on these numbers, Harvard spokesman Clifford Stoll estimated the total economic impact was between $100,000 to $10,000,000.

4 Eisenberg et al, "The Cornell Commission: On Morris and the Worm."

5 Michael Rustad and Diane D'Angelo, "The Path of Internet Law: An Annotated Guide to Legal Landmarks," in *Duke Law & Technology Review 2011*, ed. Beatrice Hahn (Durham: Duke University School of Law, 2011).
6 United States v. Morris, (2d Cir. 1991), upholding the conviction of a computer science graduate student under the Computer Fraud and Abuse Act.
7 *Hearing before Committee on Governmental Affairs, US Senate* (March 2, 2000) (testimony of James Adams, Chief Executive Officer Infrastructure Defense, Inc).
8 Adam Elkus, "Moonlight Maze" in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.*
9 Ryan Richard Gelinas, "Cyberdeterrence and the Problem of Attribution," (master's thesis, Georgetown University, 2010), http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/historical/gelinasRyan.pdf.
10 Marcia McGowan, "15 Years After Presidential Decision Directive" (PPD) 63," *Booz Allen*, May 22, 2013, http://www.boozallen.com/content/boozallen/en_US/media-center/company-news/2013/05/15-years-after-pdd63-blog-post.html.
11 "Moonlight Maze," *Frontline*, PBS, April 24, 2003, www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/.
12 Office of the Press Secretary, "Fact Sheet: Protecting America's Critical Infrastructures PDD 63," May 22, 1998, http://fas.org/irp/offdocs/pdd-63.htm.
13 Ibid.
14 Ibid.
15 Kim Zetter, *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon* (New York: Crown Publishing, 2014).
16 Ralph Langner, "Stuxnet's Secret Twin: The real program to sabotage Iran's nuclear facilities was far more sophisticated than anyone realized," *Foreign Policy*, November 21, 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.
17 Ibid.
18 Irving Lachow, "The Stuxnet enigma: Implications for the future of cybersecurity," *Georgetown Journal of International Affairs Special Issue: Cybersecurity* (2011): 118–126.
19 For example, creating more institutions that monitor, coordinate, regulate, assess, defend, and attack.
20 Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement," *Council on Foreign Relations*, January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.
21 Guest Blogger, "The Top Five Cyber Policy Developments of 2015: The WSIS+10 Review," *Net Politics* (blog), Council on Foreign Relations, December 22, 2015 http://blogs.cfr.org/cyber/2015/12/22/the-top-five-cyber-policy-issues-of-2015-the-wsis10-review/.
22 Federal Trade Commission "US-EU Safe Harbor Framework," July 25, 2016, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

23 Executive Order No.12333, United States Intelligence Activities (December 4, 1981), Central Intelligence Agency, https://www.cia.gov/about-cia/eo12333.html.
24 "The Organizational Arrangements for the Intelligence Community," *Federation of American Scientists*, February 23, 1996, http://fas.org/irp/offdocs/int009.html.
25 Eric Rosenbach and Aki J. Peritz, "Cyber Security and the Intelligence Community," in *Confrontation or Collaboration? Congress and the Intelligence Community*, ed. Eric Rosenbach (Harvard Kennedy School: Belfer Center for Science and International Affairs, 2009).
26 *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Security Committee*, (February 26, 2015) (statement of James R. Clapper, Director of National Intelligence). http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.
27 "Norse Intelligence Platform," Norse, http://map.norsecorp.com.
28 Kristen Eichensehr, "Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment," *JustSecurity*, March 6, 2015, https://www.justsecurity.org/20773/cybersecurity-u-s-intelligence-communitys-2015-worldwide-threat-assessment/.
29 Ibid.
30 Department of Defense, "The DoD Cyber Strategy," April 17, 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_Cyber_ Strategy_for_web.pdf.
31 Mark Pomerleau, "IC leaders: Future cyber attacks will do real damage," *Defense Systems*, September 11, 2015, https://defensesystems.com/articles/2015/09/11/ic-leaders-map-out-nation-state-cyber-threats.aspx.
32 Ibid.
33 Andrew Meola, "Cyber attacks against our critical infrastructure are likely to increase," *Business Insider*, May 26, 2016, http://www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5.
34 Ibid.
35 Ibid.
36 Aaron Brantly, "Defining the role of intelligence in cyber," in *Understanding the Intelligence Cycle* ed. Mark Phythian (London and New York, England: Routledge, 2013).
37 Ibid.
38 Richard Bejtlich, "What are the prospects for the Cyber Threat Intelligence Integration Center?" *Brookings*, February 19, 2015, http://www.brookings.edu/blogs/techtank/posts/2015/02/19-cyber-security-center-bejlich.

Lessons Learned from the "Viral Caliphate": Viral Effect as a New PSYOPS Tool?

Miron Lakomy

This paper aims to analyze still unnoticed aspects of the so-called Islamic State's cyber jihadist campaign in order to indicate its potential utility for state-sponsored information warfare. To begin with, it tends to present the most important features of the "Islamic Caliphate's" online campaign, which aims to generate the "viral effect." Moreover, the paper attempts to provide an overview of earlier military conflicts, in which the viral effect could be noticed. And finally, based on these considerations, it answers the question how viral marketing methods and mechanisms can be used as viable tools in psychological operations.

Keywords: cyber jihadism, cyber propaganda, information warfare, PSYOPS, viral effect, viral marketing

Introduction

Information warfare[1] is becoming an increasingly important aspect of contemporary military conflicts.[2] As many recent examples have proven, the manipulation of information is frequently critical to gaining an advantage over the enemy.[3] One method of doing this is through the use of psychological operations (PSYOPS),[4] which aims to influence attitudes and the behavior of hostile populations, counter enemy propaganda and disinformation, and establish credibility among the people targeted. Until the end of the Cold War,

Dr. Miron Lakomy is an assistant professor at the Institute of Political Sciences and Journalism, University of Silesia, Katowice, Poland.

these goals were usually reached through various, but rather unsophisticated methods such as loudspeakers, leaflet drops, radio programming, comic books, posters, and TV spots and bulletins.[5] A new era of information warfare emerged at the end of the twentieth century with the worldwide propagation of the Internet. Cyberspace, being a new domain of multidimensional human activities, proved to have multiple unique features, which enabled new kinds of offensive and defensive information operations.[6] The most fundamental of these operations was accurately described by W. Tecumseh Fitch: "When I consider the effect of the Internet on my thought, I keep coming back to the same metaphor. What makes the Internet fundamentally new is the many-to-many typology of connection it allows. Suddenly any two Internet-equipped humans can transfer essential information, flexibly and efficiently. We can transfer words, code, equations, music, or video anytime to anyone, essentially for free."[7]

It is well known that the use of cyberspace for information warfare is not a new phenomenon. Many early examples such as the US intervention in Iraq or the Caucasus war in 2008 indicated that cyber propaganda usually rested on adapting the means of traditional PSYOPS to the electronic environment. Instead of leaflets and loudspeakers, they frequently utilized poorly designed spam in the form of e-mails or website comments. Posters were transformed into banners and messages that were posted on defaced websites and social media sites.[8] TV bulletins emerged as videos that were released via popular hosting services such as YouTube or LiveLeak.[9] Currently, cyberspace is characterized by its massiveness (more than 3.3 billion Internet users in 2016) and its interconnectedness, which—along with the dominance of mobile devices—open much more unique and sophisticated possibilities for propaganda *sensu largo*. This has already been realized and utilized by the so-called Islamic State (IS); its spectacular cyber jihadist campaign, initiated in 2014, now has the group's major goals echoing around the world. As Christina Schori Liang put it, "IS has brought cyber jihad to a whole new level . . . This highly successful campaign is an effective tool for psychological operations and for recruitment."[10] Naturally, its online activities have become the object of extensive scientific studies. It is therefore surprising that academics have not yet observed that in order to increase its efficiency, IS propaganda exploits techniques and mechanisms specific to viral marketing.

In this context, this study has three goals. First, this study will present the most important features of the "Islamic Caliphate's" online campaign, which generate the "viral effect." Second, this study will provide an overview of earlier military conflicts, in which the viral effect could be spotted. Third, based on these considerations, this study will answer how viral marketing methods and mechanisms can be used as viable tools in psychological operations. To summarize, the paper aims to analyze still unnoticed aspects of the IS cyber jihadist campaign in order to indicate its potential utility for state-sponsored information warfare. To achieve these objectives, the paper has been divided into three sections. The first section attempts to characterize the phenomenon of the viral effect from the perspective of its potential usability for psychological operations. The second section presents a short overview of conflicts in which propaganda went viral. Finally, the last part focuses on the "viral caliphate," i.e., the reasons why the viral effect is so evident in IS's cyber jihadist activities.

Defining the Viral Effect

The viral effect is a subject of in-depth marketing research, which has discovered that cyberspace enables the development of the well-known mechanism "word-of-mouth." It can be defined as the use of influencers "to generate peer-to-peer product recommendations or buzz."[11] Historically, word-of-mouth was strictly dependent on direct, physical contact between peers, which limited its geographical coverage and message proliferation rate.[12] In the information revolution era, word-of-mouth has evolved into viral marketing, which is defined by Maria Woerndl and others as "the transmission of marketing messages through various Internet-based channels by peers. During these transmissions, information passes between individuals without the involvement of the original message source, propagating like a virus would have done, infecting the hosts."[13] Viral marketing techniques therefore aim to incite the "viral effect," which can be broadly defined as a process of the exponential proliferation of a message online, in which individuals "infected" by its content share it with their peers through their electronic environment. The form of such a message varies, starting from simple e-mails, websites, pictures (e.g., "memes"), to games, videos, music, and documents. In principle, almost any form of uncommon content under appropriate conditions may inspire individuals to propagate it among their

friends, associates, and family. The term "viral marketing" was coined by Steve Jurvetson and Tim Draper to describe the dynamic expansion of Hotmail in 1996, which had advertised its services in the outgoing e-mails of its users. It had allowed the company to grow twenty-four times larger over a one-year period.[14] In the twenty-first century, viral marketing techniques have focused mostly on the use of short, interesting, and unconventional videos. One of the first advertisement campaigns to do so was by the blender manufacturer, BlendTec, which had prepared a series of online videos entitled "Will it blend?" It presented tests of its products using unusual items, such as expensive smartphones, wooden boards or watches. This unique approach to advertising hit the mark, as the series went viral. BlendTec's YouTube account quickly became very popular (200,000 subscribers in 2009) and retail sales jumped by 700 percent.[15] Since then, many companies have tried to use viral marketing techniques; however, very few have succeeded. The Red Bull Space Jump, Old Spice's "I'm on a Horse," and the LG Elevator Prank are worth mentioning.[16]

The viral effect is not only limited to professional advertisements; the same mechanics are exploited by hobbyists and amateurs. In fact, a large part of the "going viral" content is created purely "for fun" and not for profit, released on social media, such as YouTube, Facebook, Reddit, Twitter, Instagram, Tumblr or their national equivalents (e.g., VKontakte). Most involve random, usually ridiculous, interesting, unusual, emotional or appalling events and situations, which attract the interest of the netizens who are ultimately responsible for their further propagation among their peers. Others contain unusual references to mass culture.[17]

In this context, it must be emphasized that the features that constitute the viral effect could theoretically be used to increase the scope and efficiency of psychological operations. To begin with, the viral effect ensures the fast and exponential proliferation of messages, reaching diverse groups due to the specificity of multilayered interactions in social media. This is impossible with traditional PSYOP methods in cyberspace. Moreover, going viral is also elusive and inexpensive in nature as the transmission of messages depends strictly on the receivers, who are always important for online propaganda during military conflicts.[18] Finally, viral marketing methods, compared to both traditional advertising and classic PSYOP techniques, can also be seen

as less interruptive and more credible, thus limiting the possible negative effects of a propaganda campaign.[19]

In order to increase the chances of the occurrence of the viral effect in PSYOPS, a number of conditions should be considered. To start with, its appearance is dependent on the content of the message, which needs to be presented in an easily receivable, interesting, and unconventional form. Humor, violence, and sexuality are usually the themes that can influence individuals to transmit the message, as they are the easiest way to arouse emotions.[20] This feature is crucial for information warfare, as emotion can "infect" recipients with an idea and encourage them to disseminate it. Furthermore, although the viral effect was successfully tested in Web 1.0, containing mostly static content ("read-only web"),[21] nowadays it is strictly dependent on the sophisticated use of social networking. Thanks to the popularity of such services as Facebook, Twitter, Instagram or YouTube, and the interconnection ("share" function) that they enable, the message—if interesting enough—can proliferate exponentially and almost instantly reach audiences worldwide. Just one share on a popular social media account may encourage thousands or even millions to click the link.[22] This is strictly connected to the broader issue of the network topology, which obviously influences the spreading of information. As Romualdo Pastor-Satorras and Alessandro Vespignani stressed, "the typology of the network has a great influence in the overall behavior of epidemic spreading. The connectivity fluctuations of the network play a major role by strongly enhancing the infection's incidence."[23] There is a difference, however, in virus and information proliferation; according to Albert-László Barabási and others, the information spreads purposefully, whereas the virus does not, and thus, it represents a more complex behavior.[24] Moreover, viral efficiency depends on the level of the information and communications technology (ICT) development of the country/society being targeted. Electronically underdeveloped nations are less susceptible to online propaganda. Simultaneously, societies that are highly dependent on electronic communication pose a more suitable target as the manipulative message will have a bigger chance to actually "go viral," due to the quantity and quality of online interactions. And finally, the population being targeted may be less keen to use the Internet in an ordinary manner during a crisis or conflict as their interests will be drawn away from everyday online activities. Moreover, audiences may be much more suspicious of unknown online content. Thus,

the viral effect theoretically should be more difficult to achieve. As the Arab Spring experiences suggest,[25] however, even during serious crises, people tend to use electronic communication extensively for information collection or coordination purposes. That is why in most situations, it should still be possible to generate a viral effect that would resonate throughout the targeted societies' electronic environment.

In summary, viral messages, whether for profit or non-profit, amateur or professional, are unconventional in nature and stand out amongst the plethora of Internet content, which is the key to their popularity. They frequently transgress typical online communication methods, therefore attracting the attention of Internet users. The viral effect refers to appealing to the interest of the Internet users in order to "infect" them with a concept, idea or brand, which then should be transferred to other users through the wide spectrum of social media channels. As a matter of fact, without the use of contemporary social media and various interconnected applications a trend of this scale would be virtually impossible. As a result, viral messages have emerged as a new and powerful phenomenon in online communication. By exploiting emotions and curiosity, they can visibly affect the way Internet users see various issues and act offline, which, in certain circumstances, can be utilized by skillful psychological operations.

Information Warfare Goes Viral

Given the aforementioned considerations, it should be noted that the viral effect is nothing new in the online dimension of wars. Since the beginning of the twenty-first century, armed conflicts have been accompanied by cyber propaganda, mostly due to the propagation of mobile devices with cameras—such as smartphones—and the development of Web 2.0 technologies.[26] As a result of these two developments, the Internet became flooded with pictures and movies documenting various wartime events. Naturally some of them proved to be so uncommon that they managed to go viral to various degrees. A few early examples occurred during the US invasion of Iraq in 2003 and the Caucasus war in 2008. The real change, however, began during the Arab Spring, which proved the utility of social media for influencing political attitudes and the morale of populations. Middle Eastern activists in 2011 made extensive use of Web 2.0 tools to organize themselves, promote their political agenda, and inspire populations to revolt against authoritarian

regimes.[27] It is therefore not surprising that the same political activists who participated in the Arab Spring revolutions then used their rich experience with social media to conduct propaganda during the subsequent military conflicts. With the scope of new manipulative content released online, the viral effect occurred in a number of interesting cases.

The Libyan civil war in 2011 between the western-backed rebels and Muammar Qaddafi's regime was the first case in history where social media was used to such an extent that it influenced international public opinion. Soon after the first battles broke out, the Internet was flooded with videos and pictures documenting battles against the Qaddafi regime. These videos and pictures sometimes also contained statements or manipulations aimed at gaining external support. Their technical and substantive sides were usually amateurish. Nonetheless, the viral effect was evident in two cases. The first one concerned the famous "Libyan guitar hero" picture, which quickly proliferated through the various picture-hosting services,[28] and contributed to the positive image of the Libyan rebels. Due to the unconventionality of this photo, merging two separate themes—fusillade and music—it was quickly noticed by the media, which also disseminated the message to the West.[29] In effect, the picture may have reached hundreds of thousands of netizens.

The usability of the viral effect for PSYOPS was also confirmed by the death of Muammar Qaddafi in October 2011, which was recorded from several perspectives and released online by the rebels soon after. In just a few hours, videos showing the brutal lynching of the former dictator proliferated across Internet news services and social media. They were also quickly picked up by leading TV stations such as CNN, BBC, and NBC.[30] In effect, at the time, these recordings proved to be the most popular content not only on the Internet, but also in the global media. Dozens of copies of the lynching posted on YouTube alone gathered millions of viewers. For instance, the Al-Jazeera version, released online on October 20, 2011 by the YouTuber user xciter79, was viewed over six million times by 2016. The versions posted by ABC News and Al-Arabiya each were viewed over one million times.[31] The videos presenting Qaddafi's last moments were played across the world due to the huge viral effect they had incited. The viral effect was possible because these recordings combined a few significant features. They were shocking and contained purely graphic content; yet graphic content alone would not attract people's attention as the Internet is

full of materials restricted to 18 years and over. Moreover, these recordings presented in detail the death of a widely hated dictator, which in itself was very unusual. Qaddafi's death also symbolically ended the civil war in Libya, which was closely followed by the international community. To summarize, these factors together created the biggest and the most apparent viral effect during a military conflict to date.

This lesson was quickly learned by the Syrian rebels, who started to post a staggering amount of propaganda online. While the opposition to the Bashar al-Assad regime extensively used the Web 2.0 environment to inspire national and international support, their attempts usually failed as they frequently released videos and pictures presenting their own terrorist activities or war crimes.[32] This ignorance was manifested by a video of rebel commander Abu Sakkar mutilating the corpse of a Syrian soldier and eating his flesh. In theory, as he later explained in an interview with the BBC, he did this to terrify his enemies.[33] In reality, the video actually went viral due to its unparalleled savagery. Its effects, however, were completely the opposite of what they had wanted as it deepened the West's distrust of the "moderate" rebels.

The viral effect also was apparent in the information warfare during the recent Ukrainian conflict. Although official Russian propaganda focused mostly on traditional media, such as TV stations, radio, and newspapers, Maria Snegovaya noted that hackers, bots, and trolls played an important role in promoting Russian propaganda in the online environment.[34] Pro-Russian propagandists released online manipulative videos and edited pictures throughout social media, such as VKontakte,[35] aimed at spreading fear among Ukrainian society, intimidating western nations, disrupting their perception of events, and promoting the Kremlin's agenda. Among the plethora of Russian propaganda online, the viral effect strengthened its reach in two evident cases. The first concerned a picture of an alleged Ukrainian soldier incorrectly loading the ammunition of an RPG-7. It was edited by pro-Russian propagandists[36] and released online to ridicule the war effort of Ukraine. The picture was posted on sites such as reddit.com and epicfail.com where they were viewed and shared by thousands of Internet users.[37] The second case was proof that pro-Russian propaganda also had major shortcomings. One of the "documents" released by the Russian-speaking media in cyberspace depicted the mistreatment of Ukrainian POWs in Donetsk.[38] In principle,

its aim was to damage the morale of Ukrainian society; instead, it incited a limited viral effect as it quickly proliferated throughout western Internet news services and social media, becoming a symbol of the brutality and war crimes committed by pro-Kremlin rebels.[39]

The Case of the "Viral Caliphate"

All of these examples prove three points. Firstly, the viral effect in certain circumstances can accompany psychological operations. Secondly, manipulative content may go viral without any specific intention, as a side effect of ordinary online propaganda activities. Thirdly, the propagandists do not always have any awareness of these mechanisms.

In this context, the viral effect has been used intentionally to increase the efficiency and reach of the most advanced cyber jihadist propaganda campaign ever conducted.[40] The case of the Islamic State proves that this terrorist organization has modified traditional cyber jihadist methods to increase the chances of a viral effect occurrence. The responsibility for adapting this approach rests with the dedicated PSYOP cells of the Islamic State—al-Hayat Media Center—which was created in 2014. It is composed of highly skilled professionals, such as computer graphics artists, former musicians,[41] cinematographers, editors, and manipulation experts. Despite the fact that little is known about the personnel of this group, their sophisticated and technologically impeccable multimedia products manifest their talents and knowledge. It is known that al-Hayat Media Center has two major goals. First, it attempts to win the general support of Muslim societies around the world, with special emphasis on the Middle East and Europe. This vector is evident in various ways, such as in the recruitment videos inciting audiences to join their ranks or to engage in terrorist activities in the West.[42] Second, it seeks to intimidate and confuse western societies. This vector is usually based on graphic releases presenting barbarous atrocities committed by IS members. However, as Gabi Siboni, Daniel Cohen, and Tal Koren argue, the widely publicized beheadings can also be considered part of IS's strategy targeting Muslim populations. They argue that "it is a source of attraction for potential recruits by appealing to senses of basic Islamic morality within the framework of a return to the fundamentals of early Islam."[43]

To reach these objectives, the Islamic State's propaganda machine planned its actions in cyberspace in ways of maximizing the chances of generating

the viral effect. Several arguments support this statement. First of all, IS's propaganda campaign is based on extensive and highly sophisticated use of social media.[44] In 2014 the number of accounts on Twitter alone that shared IS propaganda ranged from 46,000 to more than 70,000. On average, Twitter accounts supporting the Islamic State had about 1,000 followers each.[45] The Islamic State also utilizes other social networks, as well as peer-to-peer applications (Telegram and Surespot) and content-sharing services (JustPaste.it and Archive.org).[46] Moreover, they extensively use various video-sharing services, starting from the most popular ones like YouTube, to the more controversial LiveLeak and the Canadian shock site BestGore.com.[47] Hence, the scope and the variety of cyber jihadist activities in social media is unprecedented. This is also a key condition in generating the viral effect as social media has many entry points for the Islamic State's propaganda, thus allowing the swift transmission of messages.

Secondly, the technical side of the Islamic State's releases is virtually flawless. Their technical level is sometimes even compared to Hollywood movies.[48] Production and postproduction equipment and methods used by the al-Hayat Media Center, including videography, editing, computer graphics, sounds effects, and photography are of the highest quality. This was highlighted by Charlie Winter who argued that, "undeniably, the production effort behind *Although the Disbelievers Dislike It* was formidable. It is clear that the content of the video was carefully considered and the individual (or individuals) who directed it were obvious perfectionists . . . the equipment that IS attempted to keep out from shooting—the cameras, in particular—demonstrates the professionalism of the operation."[49] This is where the uniqueness factor comes in. The technical quality of IS propaganda distinguishes itself from other cyber jihadist productions. There is no comparison between the crude releases of al-Qaeda, al-Shabab or Boko Haram, for example, and the high definition Hollywood-style movies with multilingual translation produced by the Islamic State. Moreover, such productions match the ordinary communication habits of the western audiences. Therefore, both of these issues naturally increase the chances of the viral effect.

In comparison to the majority of cyber jihadist releases, IS frequently adopts unconventional forms of propaganda, which also draw the attention of western citizens. Messages produced by the al-Hayat Media Center frequently refer to cyber or mass culture canons. For instance, one of the

videos exploited a very popular gaming brand.[50] Other examples include the so-called #mujatweets on Twitter,[51] extensive use of memes, and the American-stylized *nasheed* music videos. These references frequently are combined with barbarous savagery, such as decapitations or corpse mutilations, which aim to generate extreme emotions. The distinct contrast between properly introduced cyber culture clichés and horrible atrocities is unique among cyber jihadist propaganda. In effect, such a convergence especially seduces youth, more efficiently than the previously dull statements that were released, for example, by Osama bin Laden. Thanks to evident references to mass and cyber culture, targeted audiences can more easily understand and embrace the message, thus enabling the viral mechanism. In summary, terrorist organizations had never before released graphic images and videos, as well as propaganda music in a way that was specifically for the western entertainment sector. This feature naturally attracts the attention of netizens, which is a crucial condition for inciting the viral effect.

The Islamic State combined the trendiest methods of online communication—social media and the most popular apps—with technological advancement, crude savagery, and manipulative sophistication on an unprecedented scale.[52] This is the key to their great propaganda "success," symbolized by the scale and proliferation of a series of videos presenting decapitations of western citizens (e.g., James Foley, Steve Sotloff, David Haines, and Alan Henning). These beheadings, published from August 2014 onwards, went viral on a global scale shortly after their initial online release. A few features contributed to their viral effect: the aforementioned technical flawlessness; the sheer brutality they presented; and the sophisticated manipulative content, evident in the statements by the prisoners and by "Jihadi John." Finally, they all exploited the same video-sharing services, including YouTube, LiveLeak, BestGore, and other social media, which ensured their instant proliferation on the Internet. Basically, they combined the uniqueness factor with professional propagation via multiple social media entry points.

In effect, these beheading videos have become the most successful pieces of viral terrorist propaganda in history. Several arguments support this statement. First, it is difficult to assess exactly how many people have viewed or heard about these videos,[53] but tens of millions is the lowest possible estimate. This is due to the fact that there were two interconnected proliferation vectors for this campaign. They have gone viral through social

media and video-sharing services. Although administrators frequently deleted the original releases, edited or intact copies proliferated instantly over the web, supposedly due to the activities of unaffiliated netizens. YouTube alone still contains dozens of Islamic State's censored decapitation recordings viewed by millions of Internet users. The two most popular copies of James Foley's execution, which were published on YouTube, were viewed almost four million times by May 2016. Its full version posted on LiveLeak has been viewed more than one million times.[54]

Journalists also quickly spotted these videos. As a result, leading global media, both offline (via TV news) and online (through official YouTube accounts and dedicated websites) released censored and shortened recordings with commentary in hundreds or even thousands of copies. Many also prepared their own reports on the executions, which frequently contained excerpts of the manipulative statements included in the original videos. This trend was visible just after the first release of James Foley's execution when all the offline and online global media outlets were full of its screenshots, edited recordings, and detailed descriptions. A google video search of the words "James Foley" has about 322,000 hits, frequently related to his execution. It should be emphasized that both these vectors were self-perpetuating. While the media reports increased the curiosity among netizens in the original videos, the popularity of the unedited versions escalated viewers' interest in successive media reports; thus the media unwittingly contributed to the success of the Islamic State's PSYOP. Thanks to them, audiences could know what the Islamic State wanted to tell them, even if they did not see the original recordings.

Furthermore, the viral aspect of the IS beheadings is manifested by the popularity of this theme among the blogosphere pundits and amateurs, creating a multitude of content referring to IS atrocities. These include various analyses, commentaries, and even parodies. The scope of this trend is exemplified by the popularity of the YouTube movie, "ISIS Bloopers," a pastiche of the famous executions prepared by Israeli comedians. Between February 2015 and May 2016, it was viewed more than 5.2 million times.[55] The abundance of amateur-made content referring to IS decapitations proves that this "epidemic" factor has really worked. If it had not worked, Internet users would not devote their time and resources to preparing their own materials that mention these events.

It must be stressed that the exposure of millions of western citizens to the unusual IS decapitations, which went viral online and offline and were strengthened by alarming reports from the Middle East and by terrorist attacks in Europe, have contributed to the increasing fear of the Islamic State, especially in the West. The success of the Islamic State's propaganda is evident in the statistics of the Pew Research Center, which indicate that western societies perceive the Islamic State as the top global security threat.[56]

Conclusions

The activities of the "viral caliphate" pose a serious threat to international security, including, among others, an increased risk of micro terrorism, as well as a deepening fear and confusion among western nations. Therefore, the information security policies of the NATO/EU states aim to quickly suppress this feature of the Islamic State's cyber strategy.

Paradoxically, the Islamic State's success also allows several conclusions to be drawn about the usability of the viral effect in psychological operations. Firstly, there is no certainty that a message designed to go viral in PSYOP will ever do so. The tapestry of human relations on various levels in the Internet is too dynamic and elusive to exploit it successfully every time. Designing actions that will meet the constantly changing features of online communication, including varying trends and moods of netizens, is highly problematic. As David Meerman Scott states, "nothing is guaranteed to go viral."[57] From thousands of IS messages released online in the form of videos, music, statements, banners, and memes, only a few actually have gone "epidemic."

Secondly, the case of the "viral caliphate" shows how important it is to conduct proper cyber reconnaissance. Adapting a message to the targeted group's "cyber cultural" background as well as to the level of ICT development increases the chances of the viral effect. Thirdly, PSYOP intending to exploit this effect should use multiple "vectors of attack," both in terms of content and technology. One message posted online has little chance of going viral. A hundred messages in various forms may sometimes make a difference, as the probability of attracting the audience's attention will increase. This is understood by the al-Hayat Media Center, which has flooded the Internet with its propaganda. Moreover, these messages should be proliferated throughout a wide range of channels: websites, social media networks, and

other online services, including those that are the most popular among the targeted population.

Fourthly, viral campaign should both precede and coincide with political and military events, which was evident in the aforementioned executions, in which "Jihadi John" referred to President Obama's statements. Anticipation may minimize the chances of the messages being recognized as hostile propaganda by the targeted populations. At the same time, messages should strictly refer to the most important events for PSYOP. Such a solution may strengthen operational efficiency as it draws attention to messages that are up-to-date and controversial or unusual. This was also done in the infamous execution videos. Fifthly, the case of the "viral caliphate" proves that the message inciting the viral effect should be in compact form and be easily accessible, meaning that it must not require any logins, passwords, web browser add-ons or plug-ins. This is due to the fact that users usually are not keen to log in or install new software in order to familiarize themselves with even the most interesting online content. Moreover, content should be simply named, in a way that will increase the chances of finding it through social media or search engines. In the Web 2.0 environment this also heavily depends on the use of proper hashtags (#), such as IS's #mujatweets.

And finally, the content of the message should be as intriguing, unconventional, and unique as possible. This does not mean that PSYOP should just copy classic viral marketing techniques frequently based on sexual themes. Instead, humor and violence presented in a unique and unconventional form—both used by the Islamic State—may be the right way to go. Humor may be more elastic, and, if used properly, can spark various reactions from the audiences, both positive and negative. For instance, al-Hayat Media Center frequently mocked the American military effort in the Middle East, using humor as a tool. Violence also may have a different role as it may shock and intimidate recipients; this was carried out perfectly in many of the execution videos posted online by the Islamic State.

In conclusion, the case of the "Islamic Caliphate" and the aforementioned military conflicts suggest that the viral effect can be efficiently exploited by psychological operations in cyberspace. Although it is a highly uncertain tool, with enough deliberation, it is possible to increase the chances of its occurrence and gain outstanding benefits for its creators, as proven by the case of the infamous IS executions.

Notes

1 Brian Nichiporuk defined information warfare as "the process of protecting one's own sources of battlefield information and, at the same time, seeking to deny, degrade, corrupt, or destroy the enemy's sources of battlefield information." According to Nichiporuk, information warfare includes operational security, electronic warfare, psychological operations, deception, physical attack on information processes, and information attack on information processes. See Brian Nichiporuk, "U.S. military opportunities: information-warfare concepts of operation," in *Strategic Appraisal: The Changing Role of Information in Warfare*, eds. Zalmay Khalilizad, John White, and Andy W. Marshall (Santa Monica: RAND Corporation, 1999), p. 180.

2 See, for example, Catherine E. Theohary, "Information Warfare: The Role of Social Media in Conflict," *CRS Insights*, March 4, 2015; Scot Macdonald, *Propaganda and Information Warfare in the Twenty-First Century* (New York: Routledge, 2007); Edward Lucas and Ben Nimmo, "Information Warfare: What Is It and How to Win It?" *CEPA Infowar Paper*, no. 1 (2015); Margarita Jaitner and Peter A. Mattsson, "Russian Information Warfare of 2014," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, eds. Markus Maybaum, Anna-Maria Osula, and Lauri Lindström (Tallinn: NATO CCD COE, 2015); William Hutchinson, "Information Warfare and Deception," *Informing Science* 9 (2006): 213–223.

3 See Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Santa Barbara: Praeger, 2013); Thomas Eljker Nissen, "Terror.com—IS's Social Media Warfare in Syria and Iraq," *Contemporary Conflicts* 2, no. 2 (2014).

4 Carnes Lord, "The Psychological Dimension in National Strategy," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, eds. Carnes Lord and Frank R. Barnett (New York: National Defense University Press, 1989), pp. 13–14.

5 See Headquarters, Department of the Army, *Psychological Operations Tactics, Techniques, and Procedures*, FM 3-05.301 (FM 33-1-1), (Washington, DC, December 2003).

6 See, for example, Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica: RAND Corporation, 1996); Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

7 W. Tecumseh Fitch, "Evolving a Global Brain," in *How is the Internet Changing the Way You Think?* ed. John Brockman (New York: HarperCollins, 2011), p. 184.

8 See James Joyner, "Competing Transatlantic Visions of Cybersecurity," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington DC: Georgetown University Press, 2012); Giorgi Targamadze, *Information Warfare against Georgia* (Tbilisi: Georgian Foundation for Strategic and International Studies, 2014); Michael

Kofman, and Matthew Rojansky, "A Closer look at Russia's 'Hybrid War,'" *Kennan Cable*, no. 7 (2015).

9 Cori E. Dauber, *YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer* (Carlisle, PA: US Army War College, Strategic Studies Institute, 2009).

10 Christina Schori Liang, "Cyber Jihad: Understanding and Countering Islamic State Propaganda," *GSCP Policy Paper*, no. 2 (2015), p. 2.

11 MindComet Corporation, *Viral marketing: Understanding the Concepts and Benefits of Viral Marketing*, The Relationship Agency White Paper (2008), p. 3, http://cmginteractive.com/uploads/viral_marketing.pdf.

12 Ibid.

13 Maria Woerndl, Savvas Papagiannidis, Michael Bourlakis, and Feng Li, "Internet-induced Marketing Techniques: Critical Factors in Viral Marketing Campaigns," *International Journal of Business Science and Applied Management* 3, no. 1 (2008), p. 34.

14 Victoria Fairbank, "A Study into the Effectiveness of Viral Marketing over the Internet," (University of Gloucestershire, 2008), pp. 12–13, http://ct-files.glos.ac.uk/mwd/modules/co333/showcase/MU303_08_FairbankV.pdf,; Steve Jurvetson and Tim Draper, "Viral Marketing: Viral Marketing Phenomenon Explained," *DFJ*, January 1, 1997, http://dfj.com/news/article_26.shtml.

15 Christian Briggs, "BlendTec Will It Blend? Viral Video Case Study," *SocialLens*, January 2009, http://www.socialens.com/wp-content/uploads/2009/04/20090127_case_blendtec11.pdf.

16 Laura Crimmons, "Top Viral Marketing Campaigns of All Time," *Branded3*, December 2, 2014, https://www.branded3.com/blog/the-top-10-viral-marketing-campaigns-of-all-time/.

17 This kind of viral content sometimes contributes to the global cyber culture. One of the greatest examples of this trend concerns a set of popular comic-style meme pictures, which went viral several years ago, influencing communication habits in social media worldwide. One can mention "Neil deGrasse Tyson reaction," "forever alone," "trollface" or "Yao Ming face." See "Neil deGrasse Tyson reaction," Knowyourmeme, http://knowyourmeme.com/memes/neil-degrasse-tyson-reaction; "Forever alone," Knowyourmeme, http://knowyourmeme.com/memes/forever-alone; "Trollface / Coolface / Problem?" Knowyourmeme, http://knowyourmeme.com/memes/trollface-coolface-problem, "Yao Ming Face," Knowyourmeme, http://knowyourmeme.com/memes/yao-ming-face-bitch-please.

18 Woerndl and others, "Internet-Induced Marketing Techniques," pp. 35–36.

19 MindComet Corporation, *Viral marketing*, p. 4.

20 Petya Eckler and Shelly Rodgers, "Viral Marketing on the Internet," in *Wiley International Encyclopedia of Marketing*, eds. Jagdish N. Sheth and Naresh K. Malhotra (New York: Wiley, 2010), http://onlinelibrary.wiley.com/doi/10.1002/9781444316568.wiem04009/pdf.

21 For more about Web 1.0, see Sareh Aghaei, Mohammad Ali Nematbakhsh, and Hadi Khosravi Farsani, "Evolution of the World Wide Web: From Web 1.0 to Web 4.0," *International Journal of Web & Semantic Technology* 3, no. 1 (2012): 1–10.

22 This mechanism is simple; source accounts share the message among followers, and then their followers can transmit the message further to their followers, and so forth.

23 Romualdo Pastor-Satorras and Alessandro Vespignani, "Epidemics and Immunization in Scale-Free Networks," in *Handbook of Graphs and Networks: From the Genome to the Internet* eds. S. Bornholdt and H.G. Schuster (Wiley-VCH, Berlin, 2002), p. 19, http://arxiv.org/pdf/cond-mat/0205260.pdf.

24 Albert-Lászlo Barabási, Dashun Wang, Zhen Wen, Hanghang Tong, Ching-Yung Lin, and Chaoming Song, "Information Spreading in Context," in *Proceedings of the 20th International Conference on World Wide Web* (Hyderabad: 2011), p. 2, http://www.barabasilab.com/pubs/CCNR-ALB_Publications/201102-10_WWW-Spreading/201102-10_WWW-Spreading.pdf.

25 See Mirosław Lakomy, "Arab Spring and New Media," in *The Arab Spring*, ed. Beata Przybylska-Maszner (Poznań: Wydawnictwo Naukowe WNPiD UAM, 2011).

26 See Dauber, *YouTube War*; Pew Research Center, *Social Networking Popular Across Globe: Arab Publics Most Likely to Express Political Views Online*, Global Attitudes Project, (December 12, 2012), http://www.pewglobal.org/2012/12/12/social-networking-popular-across-globe/.

27 See, for example, Mikael Eriksson and others, *Social Media and ICT during the Arab Spring*, no. FOI-R--3702--SE (Swedish Defence Research Agency July 2013); Lakomy, "Arab Spring and New Media."

28 "Man plays a guitar in the middle of a shootout in Libya," *Imgur*, http://imgur.com/r/HumanPorn/pyMmP.

29 See Uri Friedman, "Libya's Fighting Guitar Heroes," *Atlantic*, October 12, 2011, http://www.thewire.com/global/2011/10/libyas-fighting-guitar-heroes/43584/; "The story behind the Libyan guitar hero photo," *Channel 4*, http://www.channel4.com/news/the-story-behind-the-libyan-guitar-hero-photo; Lee Moran, "Now that's a real guitar hero: Libyan soldier strums away as battle for Sirte rages around him," *Daily Mail*, October 11, 2011, http://www.dailymail.co.uk/news/article-2047889/Libyan-soldier-strums-guitar-battle-Sirte-rages-him.html.

30 See Moni Basu and Matt Smith, "Gadhafi killed in crossfire after capture, Libyan PM says," *CNN*, October 21, 2011, http://edition.cnn.com/2011/10/20/world/africa/libya-war; "Libya's Col Muammar Gaddafi killed, says NTC," *BBC News*, October 20, 2011, http://www.bbc.com/news/world-africa-15389550; "Libya's Moammar Gadhafi killed in hometown battle," *NBC News*, http://www.nbcnews.com/id/44971257/ns/world_news-mideast_n_africa/t/libyas-moammar-gadhafi-killed-hometown-battle/#.VyJ7k-SbSUk.

31 "Gaddafi death," *YouTube*, https://www.youtube.com/results?search_query=gaddafi+death.

32 "Syria," *YouTube*, accessed April 9, 2016, https://www.youtube.com/results?sp=CAM%253D&search_query=syria&page=1&nohtml5=False.

33 Paul Wood, "Face-to-face with Abu Sakkar, Syria's 'heart-eating cannibal,'" *BBC News*, July 5, 2013, http://www.bbc.com/news/magazine-23190533.

34 Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Institute for the Study of War, September 2015), pp. 13–14, http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

35 Myroslav Shkandrij, "How Russian Propaganda Works Through Social Media," *Myroslav Shkandrij's Blog*, May 9, 2014, http://www.ukrainianwinnipeg.ca/russian-propaganda-works-social-media/.

36 Original photo at *Imgur*, http://i.imgur.com/BuiPsTj.jpg.

37 "It's Gonna be a Short War," *Epic Fail*, December 31, 2015, http://www.epicfail.com/2015/12/31/its-gonna-be-a-short-war/; Reddit, https://www.reddit.com/r/pics/comments/3kh4o3/sorry_captain_i_am_of_still_learnings_how_to/.

38 See "UAF Storm Donetsk Airport and Get their Assess Handed to them by NAF. FULL VERSION [Warning: Graphic]," *YouTube*, https://www.youtube.com/watch?v=3TZ9Q18HKlQ.

39 See "Ukraine rebels launch grisly propaganda war," *France24*, http://observers.france24.com/en/20150128-ukraine-rebels-launch-grisly-propaganda-war.

40 See Christina Schori Liang, "Cyber Jihad: Understanding and Countering Islamic State Propaganda," *GSCP Policy Paper*, no. 2 (2015); Adam Hoffman and Yoram Schweitzer, "Cyber Jihad in the Service of the Islamic State (ISIS)," *Strategic Assessment* 18, no. 1 (2015): 71–81; Erin Marie Saltman and Charlie Winter, *Islamic State: The Changing Face of Modern Jihadism* (London: Quilliam Foundation, 2014); Yannick Veilleux-Lepage, "Paradigmatic Shift in Jihadism in Cyberspace: The Emerging Role of Unaffiliated Sympathizers in Islamic State's Social Media Strategy," *Journal of Terrorism Research* 7, no. 1 (2016): 36–51, http://doi.org/10.15664/jtr.1183.

41 See Hayley Cole, "German rapper turned extremist behind Islamic State beheading videos and uses music to recruit young jihadis," *Mirror*, November 9, 2014, http://www.mirror.co.uk/news/uk-news/deso-dogg-german-rapper-turned-4597188.

42 For more on the topic, see Gabi Siboni, Daniel Cohen, and Tal Koren, "The Islamic State's Strategy in Cyberspace," *Military and Strategic Affairs* 7, no. 1 (2015): 127–144; Charlie Winter, *Documenting the Virtual 'Caliphate'* (London: Quilliam Foundation, 2015).

43 Siboni, Cohen, and Koren, "The Islamic State's Strategy in Cyberspace," p. 137.

44 Charles Lister, "Profiling the Islamic State," *Brookings Doha Center Analysis Paper*, no. 13 (2014), p. 3, https://www.brookings.edu/wp-content/uploads/2014/12/en_web_lister.pdf; Veilleux-Lepage, "Paradigmatic Shift in Jihadism in Cyberspace."

45 J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter," *The Brookings Project on U.S. Relations with the Islamic World Analysis Paper*, no. 20 (2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

46 Brendan I. Koerner, "Why ISIS Is Winning the Social Media War," *Wired* (April 2016), https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.

47 Miron Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw* (Katowice: Wydawnictwo Uniwersytetu Śląskiego, 2015).

48 Michael S. Schmidt, "Islamic State Issues Video Challenge to Obama," *New York Times*, September 17, 2014, http://www.nytimes.com/2014/09/17/world/middleeast/isis-issues-video-riposte-to-obama.html?_r=0.

49 Claire Davis and Charlie Winter, *Detailed Analysis of Islamic State Propaganda Video: Although the Disbelievers Dislike It* (London: Quilliam Foundation and TRAC, December 19, 2014), p. 31, https://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/detailed-analysis-of-islamic-state-propaganda-video.pdf.

50 Michelle Malka Grossman, "Watch: Islamic State's terror video game," *Jerusalem Post*, September 21, 2014, http://www.jpost.com/Middle-East/IS-claims-it-created-a-terror-video-game-375935.

51 *Mujatweets*, https://twitter.com/hashtag/mujatweets.

52 Miron Lakomy, "Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?" *Studia Politologiczne* 38 (2015): 156–182.

53 Some of censored versions have been viewed on YouTube more than one million times through mid-April, 2016. See "Islamic State Execution," *YouTube*, https://www.youtube.com/results?search_query=islamic+state+execution, accessed April 14, 2016.

54 "James Foley," *YouTube*, https://www.youtube.com/results?q=james+foley&sp=CAM%253D; "James Foley," *LiveLeak*, http://www.liveleak.com/browse?q=james%20foley&sort_by=views.

55 "ISIS Bloopers," YouTube, https://www.youtube.com/watch?v=Qz3oWmDUW1Q.

56 Jill Carle, *Climate Change Seen as Top Global Threat* (Pew Research Center, July 14, 2015), http://www.pewglobal.org/2015/07/14/climate-change-seen-as-top-global-threat/.

57 David Meerman Scott, *The New Rules of Viral Marketing: How word-of-mouse spreads your ideas for free* (n.p., 2008), p.16, http://www.davidmeermanscott.com/hubfs/documents/Viral_Marketing.pdf?__hstc=17524326.4476318ded53d9884be8e803282f82b2.1472783930977.1472783930977.1472783930977.1&__hssc=17524326.2.1472783930978&__hsfp=3082634171.

An Intelligence Civil War: "HUMINT'" vs. "TECHINT"

Matthew Crosston and Frank Valli

Since 9/11, intelligence has evolved within a changing atmosphere of modern tactics and techniques for information collection. This atmosphere, coupled with massive leaps in technological advancement such as social media, mobile communications, processing analytics, large-form solid-state data storage, novel computational hardware, and software equipment, has thrust intelligence communities around the world into a strange new world of multi-dimensional intelligence. While science and technology and human capability both remain valuable facets of the same overlapping intelligence construct, there is an emerging trend of diametrically opposed camps pushing for one method over the other. This article explains how in terms of field application and intelligence information processing and analysis, both HUMINT and TECHINT could be maximized by the elimination of forced rivalry and by the encouragement of mutual cooperation that is currently lacking.

Keywords: cyber, intelligence, TECHINT, HUMINT, science and technology, national security

An earlier version of this paper was published by Frank Valli as "'HumInt' vs. 'TechInt': A Forced Intelligence Dichotomy," *The Security and Intelligence Studies Journal* 1, no. 3 (Summer 2014). Parts of this paper were also published in Matthew Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies," *New Eastern Outlook* (April 3, 2015).

Dr. Matthew Crosston, professor of political science, is the director of the International Security and Intelligence Studies (ISIS) program at Bellevue University. Frank Valli earned a Master of Science degree in the International Security and Intelligence Studies program at Bellevue University.

Introduction

Since 9/11, intelligence has evolved within a changing atmosphere of modern tactics and techniques for information collection. This atmosphere, coupled with massive leaps in technological advancement—such as social media, mobile communications, processing analytics, large-form solid-state data storage, novel computational hardware, and software equipment—has thrust intelligence communities around the world into a strange new world of multi-dimensional intelligence. With the implementation of new technologies and their expansion into the public arena, intelligence collection methods—once reserved specifically for governments or major conglomerations—have increased far beyond traditional human intelligence capability. Countering this, however, and setting the stage for the examined tension, is the admission that humans must not be "devolved" from the field of intelligence. No matter how technologically advanced war may become, human assets will remain paramount in some form or other. "Human Intelligence" (HUMINT) should thus always be considered first among equals.

All these advances have been utilized extensively by the intelligence community in the past and now find themselves freely available for public use. Moreover, the more recent controversial revelations involving metadata usage for threat assessment and identification—in short, the entire Snowden affair—can also be included in this encroachment of the technological into the HUMINT sphere. Techniques taught nowadays to university students for conducting rigorous quantitative research (such as mixed-methods software, automatic computer coding, content analysis, text mining, and bootstrapping), in the previous generation would have been hard-to-access technology found almost exclusively within government circles. The incorporation of science and technology into the loosely termed "Technical Intelligence" (TECHINT) has become a major contributor to both data and strategy.[1] While science and technology and human capability remain valuable facets of the same overlapping intelligence construct, an emerging trend sees diametrically opposed camps pushing for one method over the other. This article explains how in terms of field application and intelligence information processing and analysis, both HUMINT and TECHINT are maximized by mutual cooperation that is currently lacking; their forced rivalry must, in our opinion, be eliminated. Most importantly, the failure of developed countries to focus on the TECHINT/HUMINT fusion will create future national security

problems far more complicated and challenging than presently anticipated, especially as other countries around the world seem to be more motivated and accepting of this need for fusion.

A Snapshot of the TECHINT and HUMINT Relationship

As can be seen in modern theater tactics, human intelligence collection techniques are still readily employed in intelligence operations. The professional adaptation to newer scientific techniques of collecting information has indeed been challenging. Though advantageous for seasoned and novice collectors alike, there remains a highly-opinionated bias against "purely" scientific methods of information collection. This bias is most pronounced at the operational and field levels where priority is still placed on the value of spontaneous decision-making, which is supposedly unique to human collectors. On the other hand, critics ask whether it is worth risking a combatant when similar information may be collected through the technological advancements so prevalent in today's modern society: drones, listening devices, sensors, imagery, intranet infiltration, email tracking, and remote computer commandeering. The rivalry fed by these mutual biases runs deep and prevents a much-needed cohesion between the two facets of intelligence gathering.

Perhaps the best way to highlight this tension is the example often praised as the model for TECHINT/HUMINT collaboration: drone usage. While it is true that the validated drone targets were always meant to be established initially by the effective use of human assets on the ground in the target area, the enthusiastic success of the drone program over the years has led to a relaxing of this process. Today, there are numerous TECHINT-validated drone operations on the ground ahead of time. Some parties within the intelligence community have argued that the possible occasional mistaken target is worthy collateral damage in comparison to risking human assets in the field. What is often unsaid is that part of this change in mindset is also an issue of immediacy and convenience: the need for formal HUMINT validation of targets on the ground slows down and limits drone capabilities and usage.[2] Over time, the tendency to maximize TECHINT in such cases has reduced the value placed on HUMINT and lessened the importance of proper TECHINT/HUMINT fusion.

When discussing this rivalry, a so-called knowledge inferiority complex should also be mentioned; any shift away from classic HUMINT toward TECHINT would suddenly place many intelligence professionals on the outside looking in. Worse perhaps, the requirement to upgrade one's skills from a more traditional HUMINT operative to a TECHINT specialist is likely beyond the learning curve of many seasoned veterans. This aspect of the rivalry is little discussed, possibly seen as the elephant in the room. The "science-phobia" that afflicts many universities in the West (according to which students shy away from highly technical, hard science majors[3]) has been long lamented in terms of its impact on the ability of countries like the United States to stay competitive in the global economy. But this reality also has a deep impact on the technological preparedness of young new cadres of the intelligence community. It is a two-level problem: on the one hand, there is not enough new blood capable of utilizing the tools available for intelligence collection; on the other hand, and perhaps more importantly, there do not seem to be any efforts invested in constructing a connective bridge between these two bodies of intelligence, aiming to intensify their reach and maximize talent capability.

Human Intelligence: Collection and Information

The human factor in intelligence collection is as old as war itself. In the field, it is the most readily utilizable and adaptable method for rapidly obtaining, processing, and acting on targets and objectives. The bias in favor of human information collection techniques is most evident among upper-echelon policy generators, but also among veteran field analysts and warfighters. As described in many accounts, soldiers, as "boots on the ground" for informing human intelligence, are vital to winning war.[4] According to Patrick Murphy, former chief engineer for the Defense Advanced Research Projects Agency's PM Unit of Action Technologies, "we talk a lot about technologies. In the urban warfare setting, you can't get away from the human. You can't fight urban without human."[5] This is especially applicable in the modern warfare theater that intelligence collectors face. The bias favoring HUMINT thus has a great impact on the mindset of those reading the intelligence—the recipients—especially as the intelligence is processed up the information chain to those who enact policy decisions. If there is reticence in relying too heavily on the purely technical capabilities of those who are employed by

the intelligence community, traditional policymakers and government actors (often far older than the intelligence operations agents in the field) might be even more skeptical of over-reliance on information obtained remotely from a machine rather than from a person on the ground.

Collection is only one facet of human intelligence. The information deduced from the intelligence collected is important, as it is responsible not only for formulating policy, but also for altering and developing operational capacities in the field. Human intelligence information often proves crucial for locating and neutralizing adversaries and for allowing expeditious action and reaction in the attainment of national security goals. For example, a 2013 National Public Radio broadcast on women in combat emphasized that many successful night raids in Afghanistan were the result of US servicewomen's prowess in collecting human intelligence information from Afghani women.[6] Those within the intelligence community who still favor the HUMINT bias would be justified in arguing that this would not have been possible if the command had been more focused on TECHINT capabilities and less ready to engage human operatives in sensitive and dangerous situations.

While some element of the HUMINT bias is undoubtedly based on professional self-preservation, there are still important real-war aspects in modern conflict that heighten the relevance of HUMINT capabilities. The emergence of non-state actors that blend into civilian societies, their integration, and the subsequent confusion around managing to discreetly and explicitly identify combatants and target areas have made the exclusive use of TECHINT without HUMINT messy and chaotic.[7] Advances in drone technology also illustrate this; they are not yet so sophisticated as to allow drones to fly unencumbered and unnoticed into heavily populated civilian areas and to identify and then eliminate individual targets. Hollywood movies may have gone in this direction, much to global entertainment delight, but real-world military capability is not yet there. Paradoxically, HUMINT can therefore be used to make the execution of mission objectives *less* messy and chaotic. In other words, contemporary modern warfare seems to have some aspects that ultimately make the exclusive use of TECHINT more chaotic and inefficient; the injection of HUMINT into this arena would, in fact, intensify TECHINT success ratios.

Science and Technology: Collection and Information

The employment of purely technological means for intelligence gathering is relatively new. In modern warfare, multiple high-tech devices have been added to the tools of conventional intelligence collection. Whether through email tracing, cyber collection tactics, satellite imagery analysis, or location techniques employed by drones, science and technology have provided a pivotal new capability in modern warfare with obvious technological-scientific benefits for intelligence information.[8] The assessment of the technological capabilities of terrorist groups—for example, whether they can develop and deploy "dirty bombs" or other IEDs—is a task whereby the information is analyzed most efficiently in a rigorously scientific and technological manner. Another of the most valuable benefits of TECHINT is the ability to keep operatives and warfighters out of harm's way. This benefit, however, also has its critics:

> This change from HUMINT oriented activities to a more technological approach through SIGINT fueled criticism immediately following 9/11. A number of commentators, pundits, and national security specialists argued that there was a degradation of CIA human intelligence capabilities over the past few years.[9]

Fears remain that, without human assessment of intelligence collection, subtle nuances in the data could be missed, thus leading to faulty analysis. This always is quickly countered by the idea that TECHINT can come close to being infallible because of its ease of production and the sheer quantity of data it creates. These competing narratives in assessment techniques by end users further exacerbate the antagonism between the two camps and obstruct the much-needed TECHINT and HUMINT synthesis. If this synthesis cannot take place by finding and training people to be adept in both versions of intelligence collection, then efforts should be invested in policies that encourage intelligence agencies to combine their respective emphases more coherently and effectively. Unfortunately, this encouragement has not, to date, been very strong or compelling.

TECHINT vs. HUMINT: The Policy Angle

In the past twenty years, the spawning of the digital age has created an entirely new dimension for intelligence—both in collection and information—further accelerated by 9/11, after which newly-felt American national insecurity

advanced to fever pitch. With the progression of the digital age, however, technology once reserved for agents with top-secret clearance is now available to the masses with simpler, but still powerful versions available for purchase at any computer store—be it encryption, coding, data-mining, the orgy of advanced apps free on any smartphone, or the incalculable amount of dangerous information accessible online at the mere press of a button.

Technology proliferation and transparency have created the means for massive data collection from open sources (OSINT), causing some to argue for limiting the application of HUMINT. Devastatingly for HUMINT proponents, this argument is founded on the dual hits of mission success and asset safety: if TECHINT can get the job done efficiently without human injection, why bother keeping HUMINT operation space so wide and broad?[10] The policies that previously governed intelligence collection were far from prepared to handle this new technological OSINT avalanche. The so-called graybeards of classic human intelligence techniques were confronted with a new capability for collecting quantities of information, never experienced before, while managing that onslaught effectively through traditional methods proved problematic. Forming policy in this new atmosphere and with these new capabilities has been a struggle for everyone.

Policy originating in the American intelligence community took advantage of this new scientific and technological power by exceeding the bounds of US civil liberty traditions. With the implementation of bills like the Patriot Act in 2001 and the revelations leaked by Edward Snowden in 2013, it seems that the opportunity to maximize the technical means of surveillance and information gathering is apparently too large a temptation to pass up.[11] While it is beyond the scope of this article to examine these decisions either ethically or morally, the important yet underemphasized point in society today is how these new collection capabilities have eaten away at what used to be the exclusive jurisdiction of HUMINT operatives and have intensified the bias against allegedly overpromising and underdelivering TECHINT tools. It cannot be denied that modern and advancing technology allows for greater ease of intrusion into areas and locations that were previously challenging for human agents. In addition, these same technologies aid in the development of constant and long-term surveillance and intelligence gathering. Creating such continuity with exclusively human intelligence agents was previously rather cumbersome, dangerous, and, at times, impossible.

Nobody's Happy: The Fiscal Dilemma between HUMINT and TECHINT

There has always been an economic element to this debate that is perhaps more important than most participants let on. From a fiscal standpoint for those on the HUMINT side, funding the acquisition and training of a human agent for utilization in the intelligence community can be far more beneficial. For this camp, the multipurpose utility of human agents with their analytical ingenuity and flexibility creates an appealing logic for greater investment than a cold machine that serves only one utility. This basic funding dilemma often breaks down in budgetary discussions, with one side lamenting the lack of funding to support its new "toys," while the other camp feels disenfranchised from the financial support necessary to keep its core of cadres refreshed, recruited, and reinvigorated. It can indeed be an odd dilemma, as each side is basically arguing that it does not get enough funding while claiming the other side is wasting valuable monies on less efficient practices.

This, of course, flies in the face of the fact that the annual US intelligence budget has consistently increased over the last ten years due, in great part, to the high demand for successful and relevant intelligence and the necessity for resources, ***both*** human and technological, to satisfy that demand. However, as technological development is already a large proportion of intelligence expenditure and comes with the risk of obsolescence and inadequacy in relatively short periods of time, there is a bureaucratic drive to compensate for this by focusing on "pliable" resources in the HUMINT realm. The intelligence community's long-held reputation for operating at the cutting edge of technological research and development results paradoxically in what is, at times, perceived as a massive budgetary imbalance resolved only by abandoning traditional budget alignments. As a result, TECHINT has been gaining unfair financial attention and prioritization compared to investment and support in HUMINT.

This is, however, a greatly flawed approach; budgetary priorities should be balanced effectively so that technological capabilities can benefit fundamental HUMINT techniques and tactics. This might result in reduced risk in terms of human assets being placed in harm's way while also allowing for far greater fidelity in the intelligence collected and the accuracy of subsequent analysis. Budgetary alignment for TECHINT needs to be established in a way that seeks to further advance and activate the funding given to HUMINT.

The technological battlefield that has been forecast as the war front of the future is both virtual *and* physical, whether that be with field level operatives utilizing drone capabilities or cyber analysts tracking down an electronic trail; therefore, TECHINT at its maximum efficiency and greatest relevance should be regarded as a crucial advantage for both operations and analysis. To continue the contemporary tendency to prioritize source funding in which technical capabilities are competing against human talent is to hinder intelligence capabilities and further exacerbate an unnecessary rivalry. Funding should focus on research, development, and operational efforts that fuse TECHINT and HUMINT.

Bridging the Gap

In field applications, the end goal of obtaining adequate, accurate, and actionable information is best attained when HUMINT and TECHINT capabilities are combined. Bridging this gap is no easy task as there are few collectors who operate freely within both fields, and analysts and policymakers tend to have their own preferential bias as to which intelligence capability produces the best and most reliable information and thus receives their preferential treatment, whether procedurally, bureaucratically, or financially. With the battlefield ever expanding into cyberspace and technical collection techniques, a fusion of traditional HUMINT techniques with science and technology seems inevitable.[12] This fusion should not occupy the forefront of future intelligence collection, but it should most certainly form the foundation for future recruiting techniques in terms of talent acquisition for the next generation of intelligence personnel. Eliminating prior stigmas and moving beyond dogmas of fear, be they against HUMINT or TECHINT, will be of paramount importance.

First in this effort must be the recognition that humans will never be fully eliminated from the field of intelligence. No matter how technological and scientifically advanced future warfare becomes, it will still rely on human capital in some form.[13] But the employment of scientific tools and technological capabilities to prevent threats to soldiers, increase capabilities, and present field operators with the means necessary to achieve mission goals should be considered an essential accessory to the human agent. Fortunately, the bias keeping these two INTs apart is the result of personal perspectives within the field of intelligence rather than any unsurmountable

innate dichotomy. This personal bias is founded heavily on the inadequacy that veteran operatives, skilled in traditional HUMINT techniques, attribute to the emerging importance of technology. As mentioned earlier, the fear of not being able to acquire the necessary technical skills is not based simply on their desire for job preservation, but rather on a deep philosophical and professional disagreement with how effectively and to what extent TECHINT can replace the unique advantages of human assets in the field. This is yet another reason proper fusion between the two techniques is essential. The key for short- and medium-term progress is obviously not to discard those who do not have or cannot acquire technological talent, but rather to focus on ways in which each becomes competent in the language, approaches, and objectives of the other. In this way, TECHINT and HUMINT will understand how to interact effectively, thus improving the impact of the intelligence produced and best serving national security.

The Fusion Dilemma around the World – A Brief Overview

While, for now, it is largely true that technologically-advanced states experience this self-imposed rivalry to a higher degree, the dilemma between TECHINT and HUMINT is not destined to be limited to highly-developed nations. This is a problem that will undoubtedly evolve further as intelligence practices and cooperation continue to become more of a global norm.[14] With financial and technical resource shortfalls, many less-developed countries are somewhat forced to favor HUMINT in both collection and assessment over the newer methods generated by science and technology.

Countries such as Britain, Australia, Russia, China, and Israel have begun to emphasize TECHINT over HUMINT, as can be seen by using modern intelligence staples such as drones, aerial and satellite surveillance imagery, and other MASINT, SIGINT, and IMINT tools. The same rivalry seen in the United States is likely to be seen in these countries as well, if not already evident. Countries that have progressed technologically tend to create their own internal HUMINT dilemmas within their intelligence communities, simply because scientific innovation will always outpace the ability of its people to keep up. By not finding the necessary synthesis and fusion, a country endangers its own national security, especially when many lesser-advantaged countries are willing to de facto achieve that fusion

through unscrupulous means. A brief examination of UAV (unmanned aerial vehicles) proliferation is a perfect example of this phenomenon.

De Facto Fusion in the Middle East

In 2013 the Israel Defense Forces (IDF) succeeded in destroying a drone that it tracked flying over sensitive military installations and approaching the Dimona nuclear reactor. The drone was unarmed, but operated by agents elsewhere and attempted to relay images back to a home base. The Israelis did not disclose whether the enemy objective had been successful, but they were certain that the drone was not American, Chinese, or Russian, claiming instead that it was an Iranian drone assembled in Lebanon and flown by Hezbollah.[15] We have referred to this elsewhere as the world's first "Islamic Crescent drone," and it signals the transnational nature of drone technology proliferation already in existence.[16]

In 2013, Iran claimed to have developed both Epic, a drone supposedly designed for both combat and reconnaissance, and Throne, a long-range combat UAV with alleged stealth capabilities. Iran certainly is not shy in its public relations efforts to claim regional dominance in TECHINT.[17] This should be treated with some skepticism given the Israeli factor; it is doubtful Iran can compete with the technical prowess of the Israeli military and its technical arsenal and thus some of these press releases are probably more for effect rather than actually being effective. Indeed, the general global reaction beyond Israel has been overwhelmingly skeptical. Having said that, there are still important things to consider; it is likely prudent for those who are not in favor of an assertive Iran to ascertain the veracity of its claim that its drones have dual capability—both combat and surveillance/reconnaissance.[18] Iran also has made bold claims about how it has developed the human capital to competently utilize the technology. This also needs to be verified. Not coincidentally, after these so-called Iranian "achievements," both Egypt and Saudi Arabia became far more interested in acquiring drones for their militaries and sought the necessary technical and financial investment for developing their own programs and recruiting the right amount of human capital.

The initial pursuit of tactical drones by other countries has up to now been focused much more on strategic global positioning and the projection of power in foreign policy, or at least the possible capacity of that automated

projection. Turkey, however, has a distinctly domestic aspect for its drone pursuits that could provide an extremely dangerous precedent moving forward. While it makes claims about the positive use of drones domestically in order to keep peace and resolve conflict, it seems the more immediate violent use of drones within Turkey is going to be predicated upon the continued destruction of the Kurdish Workers Party (PKK). The Turkish Army has, of course, totally avoided mentioning the PKK by name in connection to its drone policy. It instead has focused more on how effective UAVs can be with border security, urban warfare, and other operational missions. On the surface, there is very little to protest. But when one considers that these issues for years have been code words for PKK unrest, it becomes rather transparent that the deployment of armed drones within the sovereign territory of Turkey is going to be for PKK destruction. This subtle distinction shows how the need to develop human talent alongside technological acquisition is becoming ever more important as drones acquire more uses inside of territorial borders. Simple commercial-military deals like the ones Turkey and Israel had in the past are becoming more layered and spurring the acquiring countries to engage in domestic development for purely domestic security needs. It will be interesting to see how this future develops; we have seen already that there seems to be little in the way of international norms and laws to prevent global operations with armed UAVs when used by major powers like the United States. Will there be even less oversight and global community reaction when smaller powers use weaponized drones for issues taking place within their own borders? If yes, then it means the armed UAV arena moving forward is only getting deadlier with the acquisitions of countries like Turkey.

De Facto Fusion in Greater Asia

If Turkey provides a potential new precedent for armed UAVs in terms of violent domestic uses, then Singapore might also be setting a precedent as well in that it has been surprisingly explicit and direct in its long-term objectives and goals. It has openly declared the simple purchase and acquisition of UAVs from major sellers like Israel as the necessary first step in a long-range strategic plan that demands native-born and domestically-trained personnel to operate drone fleets. This is considered equally crucial, if not the more crucial strategic piece to its national plan.[19] If the Singapore

model, for lack of a better term, becomes more embraced, then the day is drawing near when more countries will be utilizing drone purchases not as the foundation of domestic fleets, but rather as the instigators to develop and evolve native industries and home-grown operators. In other words, Singapore is the country that is the most adamant in declaring its right to achieve expansive drone independence—from construction to militarization to operation capacities. If successful this will signal, if not the end, then certainly a mitigating challenge to the so-called American expertise and technological dominance.

In fact, a possibility exists that other countries within the greater Asia Pacific region will follow the Singapore model and thus create what could end up being the second largest UAV market in the world. (This fact, however, can be argued as statistical trickery: the greater Asia Pacific region *as a whole* could overtake Israel for second place. But this is conflating all national acquisitions into one whole sum. When Israel is compared to the acquisitions of individual nations of greater Asia, it maintains its solid hold in second place).[20] India, South Korea, North Korea, Malaysia, and Australia are all major actors in the greater Asian UAV market, in addition to the stalwarts of China and Singapore. Perhaps most importantly, every single one of these states have expressed the desire to not just purchase UAVs from other countries, but also to train their own agent cadres and to develop new human capital for militarized drones. These countries are pursuing the TECHINT/HUMINT fusion with greater aggression and ambition and do not feel it necessary to align their national interests to the strategic interests of the United States. Thus, it might not be wise to automatically assume that the United States need only worry about non-allies developing domestic UAV industries; even allies, pursuing their own national interests, could find themselves at odds with American objectives and policies.

This is an important distinction to make which at present is being underemphasized within UAV proliferation debates and discussions: the ability to fuse the power of TECHINT with the agility of HUMINT provides new power projection to countries that were previously limited. The United States and Israel have in the past justifiably maintained supreme confidence in their ability to outpace and outrace any other state's acquisition and development. But this logic may have been too absolutist: it is not necessary for a lesser rival to perfectly match the technical and human capabilities of

the United States or Israel in order to present real challenges and dangers to their interests. The fusion attempts described above within the drone arena show just how much potential for disaster lies in a relative increase in capability. Absolute equalization is not necessary for damage to be done.

Changing of the Guard

Retaining policy focus on the needs and requirements of the soldier, operator, and analyst will result in effective and sustainable evolutionary policy—embracing the growth of the technical field as well as the development of modern human agents—and will advance national security interests on the battlefield and in the intelligence arena. To recognize this need and adapt accordingly are the steps required for the intelligence community of the next generation.

Often the best trained, knowledgeable, and experienced personnel do not move up the rungs of the bureaucratic ladder to become effective policymakers. This lack of realistic field experience in the policymaking arena equates to a lack of successful intelligence prioritization and future innovation. As "purists" continue to dominate policy and budgetary discussions, when it comes to the TECHINT/HUMINT divide, the unnecessary and false division between these two crucially important INTs likely will continue. How do intelligence communities from countries like the United States and Israel develop beyond this? First, they should prioritize the promotion and elevation of those who see the need to integrate TECHINT and HUMINT seamlessly in both operations and policy. The only way to enact substantive change is to let people see that new approaches are being genuinely rewarded. The false dilemma over TECHINT/HUMINT can be overcome if the United States and Israel begin to promote those who see the potential of an integrated approach and produce people who are adept in the relevant tools and methodologies.

Second, the United States and Israel should begin developing their own training and educating organizations in order to produce new specialists who can walk and talk in the language and techniques of both INTs. As embarrassing as it may be to admit, there are numerous examples of this process already taking place around the world with the most obvious rivals being China and the Russian Federation. In this case, following the lead of the "enemy" may not be such a bad idea. Transitional training programs could enable and facilitate present generation intel specialists to follow and

understand the need for this fusion. There is no expectation for non-technically oriented employees to become computer scientists or technical specialists to suddenly become adroit "super spies" in the field. Rather, efforts need to be made to properly enhance and engage communication between the two communities so that they can talk and collaborate, even if each remains relatively non-proficient in the specialization of the other; it is more about facilitating competence than demanding expertise. Surprisingly, the benefit of these approaches so far has been largely overlooked. Not taking seriously the fusion between TECHINT and HUMINT as the future of intelligence means an unspoken and crippling civil war continues forward; what should become an alliance unfortunately and dangerously will remain a rivalry.

Notes

1 Intelligence Science Board, *The Intelligence Community and Science and Technology: The Challenge of the New S&T Landscape* (Washington, DC: Office of the Directorate of National Intelligence, 2010), https://fas.org/irp/dni/isb/landscape.pdf.

2 Ashley J. Tellis, *Pakistan—Conflicted Ally in the War on Terrorism* (Washington, DC: Carnegie Endowment for International Peace, 2007), http://carnegieendowment.org/files/pb56_tellis_pakistan_final.pdf.

3 Katherine Beard, "Behind America's Decline in Math, Science, and Technology," *US News & World Report*, November 13, 2013, http://www.usnews.com/news/articles/2013/11/13/behind-americas-decline-in-math-science-and-technology.

4 Andy Savoie, "Boots on the Ground: HUMINT Needed for Urban Warfare," *Aerospace Daily & Defense Report*, December 8, 2004, http://aviationweek.com/awin/official-boots-ground-humint-needed-urban-warfare.

5 Ibid.

6 "Women in Combat, and the Price They Pay," "Morning Edition," *NPR*, March 18, 2013, http://www.npr.org/2013/03/18/174444738/women-in-combat-and-the-price-they-pay.

7 WMD Commission, *Final Report of The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, DC.: Library of Congress, 2005), https://fas.org/irp/offdocs/wmdcomm.html.

8 Kevin M. O'Connell, "The Role of Science and Technology in Transforming American Intelligence," in *The Future of American Intelligence*, ed. Peter Berkowitz (Stanford: Hoover Institution Press, 2005), pp. 139–174, http://media.hoover.org/sites/default/files/documents/0817946624_139.pdf.

9 Rand C. Lewis, "Espionage and the War on Terrorism: Investigating U.S. Efforts," *Brown Journal of World Affairs* 11, no. 1 (2004):175–182.

10 Ishmael Jones, *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture* (New York: Encounter Books, 2008).
11 Public Law Pub.L. 109-177, *USA PATRIOT Improvement And Reauthorization Act of 2005* (Washington, DC: Congressional Publications, March 9, 2006).
12 Denis O'Connor, *HMRC Handling of Human Intelligence Sources.* (London: Inspectorate of HM Revenue and Customs, 2006), https://www.justiceinspectorates.gov.uk/hmic/media/hmrc-the-handling-of-human-intelligence-sources-20070325.pdf.
13 Robert K. Ackerman, "Defense HUMINT Needs Technology, Too," *Signal*, October 2006, http://www.afcea.org/content/?q=defense-humint-needs-technology-too.
14 Paul Todd & Jonathan Bloch, *Global Intelligence: The World's Secret Service Today* (New York: Zed Books, 2003).
15 Kristin Roberts, "When the Whole World has Drones," *National Journal*, March 21, 2013.
16 Matthew Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies," *New Eastern Outlook*, April 3, 2015, http://journal-neo.org/2015/04/03/american-uav-apartheid-and-the-blowback-of-new-drone-armies/.
17 East West Services, "Iran Announces New 'Epic' Combat UAV with Stealth Capability," *Geo-Strategy Direct,* May 22, 2013.
18 Crosston, "American UAV Apartheid and the 'Blowback' of New Drone Armies."
19 East West Services, "Singapore First East Asian Military to Deploy Israeli Strategic UAV," *Geo-Strategy Direct,* June 6, 2012.
20 "Asia UAV Acquisitions," *Defence Review Asia* 3*,* no.7 (2009): 20.

Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations

Gabi Siboni and Ido Sivan-Sevilla

The cybersecurity challenge cuts across fields, sectors, and approaches. This essay presents the fundamentals of the problem, embraces a risk-based approach that perceives the state as society's risk manager, and overviews the development of regulatory processes in modern societies. The essay then compares how the United States, European Union, and Israel have chosen to confront the cybersecurity challenge and stresses the importance and difficulties of imposing cybersecurity regulation on the civil sector. Finally, the essay explores some possible avenues for progress and suggests some solutions for increasing the resilience of cyberspace in the civic sector.

Keywords: regulation, risks, cybersecurity, civic sector

Introduction

Cyberspace poses various challenges on decision makers. These challenges stem primarily from the heavy dependence of states and societies on such a vulnerable sphere. While cyberspace enables the flow of information, which, in most cases, leads to economic prosperity, efficiency, and social benefits, it is also a target for national security, criminal, and commercial

Dr. Gabi Siboni is the director of the Cyber Security Program at the Institute for National Security Studies. Ido Sivan-Sevilla is a research fellow in the Cyber Security Program at the Institute for National Security Studies.

threats. The challenges to the resilience of cyberspace[1] are rooted in several key factors. First, there is an obvious asymmetry between the minimal obstacles of hackers to penetrate cyberspace and the high costs of defending it. While a successful attack needs only a single vector to advance, defense efforts aspire to cover all possible vulnerabilities. Second, cyberspace relies on outdated communications protocols, allowing attackers a great deal of anonymity and making it difficult for law enforcement agencies to identify the source of the attacks.[2] Third, cyberspace allows potential attackers to exploit the numerous hardware and software weaknesses and to use existing attack tools that succeeded in previous attacks; this phenomenon accelerates the race to defend oneself, further eroding the security level. The existence of a flourishing market to exploit zero-day weaknesses only stresses this point.[3] Furthermore, recently it transpired that commercial entities have shared software weaknesses and attacks tools with governments to facilitate spying on citizens and "regime opponents."[4]

Fourth, the lack of mechanisms to share information about cyberspace threats and the means of defense employed by commercial companies make it difficult to formulate a collective, proactive effort to prevent cyberattacks. This stems primarily from only partial information sharing and limited transparency of commercial companies in the civic sector,[5] while both the military and the state sectors fail to do their part. Fifth, there is a lack of economic incentives and technological tools to develop appropriate defense. While cyberspace damage—currently estimated in the billions of dollars—incentivizes market forces to defend themselves, most of the civic sector is not required to report data breaches and cyber threats to the state. Therefore, the cost of damage resulting from a successful breach to the reputation of a targeted company is not enough to motivate companies to protect themselves before anything happens. Alongside the growing awareness of shareholders and the customer base in the private sector, there is no inclusive or binding directive instructing companies to publish data breaches or report on the damage caused. Furthermore, the capabilities of technological tools currently available on the market are insufficient to create hermetic defenses.[6] Finally, most cyberspace users are unaware of the dangers, and provide cyberspace with sensitive, critical information that is not sufficiently protected. Many users also fall victim to social engineering attempts, choose weak passwords,

and in most cases, represent the weakest link through which systems are breached.[7]

It is therefore not surprising that we are inundated daily with reports from all over the world about newly discovered weaknesses, database breaches, sensitive information theft, and computer systems that have been maliciously damaged.[8] The ease at which commercial institutions and states collect and store critical information undercuts the efficacy of the efforts expended to protect cyberspace; thus, we find ourselves dependent on the proper functioning of a vulnerable sphere. For its part, the state tries to partially fix this market failure and intervene to either prevent cyberspace dangers from being realized or mitigate their impact after they already have occurred.

The risks posed by cyberspace are the natural progression of the risks facing the modern state, as described in 1986 by sociologist Ulrich Beck in his groundbreaking book, *Risk Society.*[9] According to Beck, modern life and its technological developments offer many opportunities, but also create new dangers to humanity and the environment. In 2002, economist David Moss referred to the complexity of risk management by governments.[10] Moss showed how the US administration, as the risk manager of the American society, went through three successive developmental stages in its risk management strategy. The process began in the nineteenth century when the United States intervened aggressively in financial risk management to encourage investments and economic growth (by legislation, such as the limited incorporation law that reduced investor risk and the early voluntary bankruptcy law that protected investors from losing everything they owned). Later, the state transitioned to risk management on behalf of workers' safety and job market stability (workers' compensation, social security, and the birth of the welfare state). Finally, in the current stage, the state manages risks for the entire society—environmental dangers, food and drug safety, and now cyberspace risks—arising from modern developments.[11]

The risk strategies that states use range from risk reduction to their distribution throughout society. On the one hand, reducing risks consists mainly of both preventing them in the first place (e.g., safety regulations, traffic signs warning to slow down, information security requirements to prevent hacking, and so forth) and mitigating the damage from a risk that has already occurred (e.g., firefighting regulations for dealing with fires,

steps to reduce the damage resulting from cyberattacks,[12] and notifying the public and state entities of a security breach so that they can protect themselves before being targeted). On the other hand, redistributing the risks consists of transferring the responsibility for the risk to a range of entities; for example, product liability laws shift the responsibility from the consumer to the manufacturer. A contemporary example is the 2015 Cyber Information Sharing Act that limits the liability for a data breach in commercial companies that choose to share information on cyber threats with the government. Risk redistribution can also occur by spreading the risks among various parties via insurance companies, for example. Every insured entity pays a certain premium to cover the damage from a risk being realized with some other party ensured under the same umbrella. In cyberspace, the private sector manages risk distribution mainly for third-party risks,[13] so far without any state intervention.

Despite the many risk strategies available, the state has not yet determined the right way to intervene—especially in the civic sector—to ensure the continuous functioning, resilience, and stability of cyberspace. In terms of the resilience of cyberspace, the civic sector has tremendous importance. Because this sector represents the lion's share of activity in cyberspace, it is exposed to most of the risks; therefore, damage to the civic sector has major economic and security implications for the resilience of the entire society, as this essay demonstrates.

State Regulation: Background and Development

At its most basic, regulation consists of control, supervision, and enforcement carried out by the state or through independent state-sponsored agencies to legally enforce binding codes of conduct.[14] It applies to those entities that the regulatory body wishes to regulate. The concept of regulation emerged in the United States at the end of the nineteenth century as a political and management method to control the economy. Regulation became the government's central tool and was a natural reaction to market failures, absence of supervision, and the emergence of so-called natural monopolies. By contrast, Europe tended to nationalize the market. Supervision through nationalization delayed the development of a regulatory tradition in Europe in tandem with the United States.[15] From the end of the 1970s and into the 1980s, the United States began expanding the use of regulation and

established independent regulatory agencies, while Europe started to use regulatory tools to accelerate its economic unity.[16]

When Margaret Thatcher was elected prime minister of the United Kingdom in 1979 and Reagan became the US president in 1981, neo-liberalism and privatization of government services were on the rise. This led to independent regulatory agencies widening the scope of their activities to regulate the market, thus giving rise to the nickname "the regulatory state."[17] The state's function has gradually shifted; from subsidizing services and helping to reduce gaps, the state now seeks to bring greater efficiency to the market by means of increased regulation (or by deregulation).[18] In practice, regulation is usually understood as legislation or sub-legislation by the state or independent regulatory agencies, expressed in binding directives, decrees, and guidelines. Its function is to control market activity, while the state sets the overall policy. In the regulatory state, experts play a key role; the demand for high expertise across issues is the initial motivation for the establishment of independent agencies.[19]

Justification for state regulation can be explained in several ways. First, regulation strives to protect the values and liberties of citizens who are liable to suffer at the hands of the powerful or from external threats. This justification explains the need for the army and security forces on the one hand, and for authorities that check and balance them on the other. Second, the economic justification for regulation is to fix market failures resulting from free market practices that do not serve the public interest,[20] e.g., the creation of a monopoly or a cartel that prices and provides products as it sees fit, making supervision necessary. Third, regulation can be justified by lack of information or asymmetry of information, which causes consumers, companies, and even states to behave in a manner inconsistent with the public good. In this case, the job of the regulatory body is to allow transparency and the free flow of information. Finally, regulation can be explained as the desire to ensure the continued existence of dwindling essential public resources that one cannot avoid using, from the quality of the air to the number of fish in the ocean. The regulatory body must ensure that these resources continue to exist, despite market forces that would—when left to their own devices—completely consume them.

The literature explains how the regulatory bodies work as part of public policy procedures and the creation of regulation in the first place using

many approaches. The theory of the public interest, also known as the functionalist theory, asserts that regulation operates to promote the common good and increase social welfare.[21] By contrast, the private interest theory maintains that private interests motivate regulatory bodies to increase the gains of centralized interest groups, usually representing a small slice of the population. In that sense, redundant regulation is a product of interest groups' relations with the state and amongst one another.[22] Furthermore, an institutional explanation for regulatory regimes can be given. An institution's capacity[23] or its historical location in the public policy process[24] explains the structuring of the regulation in the way in which it was created. In the last twenty years or so, another school of thought has emerged, which explains regulation based on ideas. According to this school of thought, paradigms play a central role in the shaping of public policy.[25] A certain idea will be perceived as "right" and as "a window of opportunity," causing decision makers to establish regulation in the spirit of the paradigm and its attendant interests.[26] In other words, in many cases, ideas and interests are intertwined to the degree that an idea can provide legitimacy and expression for interests groups, which are capable of generating regulation to serve their objectives.[27]

Regulatory Approaches in Cyberspace: Israel, the United States, and the European Union

Regulation, thus, is expanding in modern societies, and its justifications and explanations are rich and varied. Nevertheless, the literature has yet to explore the regulatory process in cyberspace. The paragraphs below describe the challenges for regulation of cyberspace, the ways in which regulatory bodies deal with cybersecurity, and how the United States and the European Union[28] have structured their regulation regimes of cyberspace compared to Israel. Finally, the essay focuses on Israeli regulation of cyberspace and highlights the largest gap in that regime—the civic sector.

Regulation in cyberspace does not refer only to defense in the classical sense; rather, it consists of many aspects directly related to national security, defense of assets and intellectual property, crime prevention, information security, and the right to privacy. Such regulatory objectives challenge regulatory bodies for three primary reasons. First, the costs involved for requiring protection are high and create vehement resistance among the private sector, which represents the largest proportion of cyberspace.[29] Second, there

is no state-issued guideline demanding that companies be transparent about their level of security and the severity of attacks in practice. Both attackers and defenders share information,[30] but generally defensive efforts do no benefit from extensive collective organizing. When commercial secrets and company reputations are at stake, it is hardly surprising that the civic sector would be unhappy to share information about the goings-on in its digital sphere. Third, regulation in cyberspace—as anywhere else—involves a conflict of interests. Most prominent are the struggles between statism[31] and liberalism, and the right to privacy versus the right to security.[32] Furthermore, struggles in the context of national security interests versus the desire for economic development (as reflected in supervision of exports of sensitive goods), as well as obstacles of information sharing among companies in light of the stringent directives issued by the director general of the Israel Antitrust Authority, serve as a partial reflection of the difficulties in instituting regulation in the field. These conflicts let loose contradicting interests and power struggles, which impede the implementation of regulation in cyberspace.

Given these challenges, regulation of cyberspace usually involves four ways of dealing with the problem of cybersecurity.[33] The most common one is to create standards and requirements in information security, including encryption, monitoring, backups, strong authentication, and so forth. In addition, regulation—especially in the United States—seeks to encourage and create mechanisms for information sharing between commercial companies and the state, based on the mutual desire to confront the problem of the lack of information and thereby protect against attacks before they occur, as well as mitigate the damage by attacks that have already occurred. The regulatory field is also notable for creating regulatory agencies and bestowing authority on state institutions to enforce defensive cybersecurity standards and practices.[34] Finally, regulatory regimes include steps to mitigate third-party hacking damage, including notifying the national CERT[35] and customers whose personal information was stolen. This is consistent with the "full circle of defense,"[36] which includes preventive steps, information sharing, and damage mitigation after an attack; together they create a coherent protective shell for organizations operating in cyberspace.

The regulatory tools used to confront cybersecurity risks generally involve legislation, binding state guidelines issued by the regulatory agencies,[37] and self-regulation by conforming to recommended standards, such as the ISO

information security standards,[38] the PCI standards for online companies providing clearing services,[39] or by internal organizational expertise, which provides guidelines for protecting the organization's computer networks, although this is not always publicly known. In addition, the state also issues standards and guidelines on the recommended way to defend the organization and/or the strategies that ought to be used. In the United States, for example, the National Institute of Standards and Technology is punctilious in issuing standards for defending and encrypting information systems,[40] while the Financial Industry Regulatory Authority assesses the best defensive cyberspace strategies for financial companies.[41]

In the Western world, there are two main approaches for states to confront cyberspace risks. While regulation in the United States is based primarily on multiple voluntary, sector-based agencies with considerable weight given to market forces,[42] the European Union presents a different, hierarchic model. Lateral institutions have strong enforcement powers, in which the state is at the center and large segments of the private sector are subject to regulation. While the United States believes that business interests will lead companies to defend themselves, the European Union takes a more interventionist approach, in which the state institution makes sure to defend the various sectors for the good of the citizens. Both the United States and the European Union enforce transparency on data breaches. In the United States, transparency is carried out at the state level (there are 47 versions of data breach notification rules),[43] whereas the European Union recently issued an upgraded General Data Protection Regulation (GDPR) Directive —effective in May 2016 and fully applied starting in May 2018—that ensures a uniform standard for notification and compensation for security breaches. The rationale of the European decision makers was to create incentives for the market to protect itself ahead of time so as not to have to bear the rigid burdens of notification and compensation.[44]

Finally, it seems that the United States is on the verge of expanding the risk strategies used, not only by preventing and mitigating damage due to cyberattacks, but also by shifting liability away from commercial companies in order to encourage information sharing. By contrast, this approach has not been adopted by the European Union and it is doubtful that it will be, given the possible infringement of the right to privacy, which the European Union views as a fundamental civil right that the state is obligated to protect. This

kind of information sharing gives legitimacy to commercial companies to increase their collecting of information and forwarding it to the state; without appropriate responsibility and transparency, it is difficult to believe this will ever be considered seriously in the European Union.

Both approaches provide only a partial solution; they do not include regulation of the state's security sector (the army, intelligence agencies, and so on), which is normally exempt from government regulation and mostly applies a self-regulation model. They also do not provide a comprehensive response for the civic sector and its multiple layers, including commercial companies, industrial institutions, and the civilians themselves.

Israel presents a hybrid model. On the one hand, the civic sector is, for the most part, not subject to any binding regulation, and, like the United States, the state relies on market forces to find the right balance between protection and economic investment. On the other hand, the statist approach is manifested in private companies, including the country's banks, in which the state dictates the information security practice because of their strategic importance. The state even imposes sanctions on such companies should they fail to meeting the necessary threshold conditions. There is an exception expressed in the Protection of Privacy Law, 1981, which includes aspects of information protection and is applied to all sectors against anyone possessing personal information; this law, however, dates from 1981, and its information protection aspects have yet to be updated.

See below the comparative chart highlighting the similarities and differences among the United States, Israel, and the European Union:

	United States	**Israel**	**European Union**
Type of regulatory regime	A liberal regulatory regime; reliance on market forces and mostly voluntary	Hybrid between liberalism and statism; critical infrastructures under state supervision; the market is driven by its own forces	A statist regulatory regime; centralized and binding
State presence	Only in critical sectors: energy, healthcare, electricity, water, etc.	Only in critical sectors: energy, healthcare, electricity, water, etc.	In critical sectors and online service providers

	United States	Israel	European Union
Risk management strategies	Progressive strategy: Prevention of cyberattacks and redistribution of liability for risks in civic sector	Solely focus on the prevention of risks. Israel has no limited liability laws with regards to cyber-security or one that requires cyber damage mitigation for companies and their customers in case of a data breach	Prevention/Mitigation of risks. Strategy of preventing attacks and mitigating damage, without redistribution of liability for company risks
Transparency towards consumers during a data breach	Exists at the state level in a non-uniform manner; 47 states, each with a different version	Non-existent	Exists in a coherent, uniform manner under Directives approved in 2016 that will be implemented by 2018
Conflict with the right to privacy	Privacy is a commodity—mostly managed by market forces, except for specific sectors (health records, information about minors, etc.)	Mostly managed by market forces, with relatively strict requirements not fully enforced by the Israeli Law, Information, and Technology Authority	Managed by the state with binding laws, institutions with power, and motivated by the interest of safeguarding privacy as a human right overriding economic interests. At the member-states level, the right to privacy is weaker vis-à-vis local intelligence agencies

Figure 1: Comparison of Cyberspace Regulatory Regimes in Israel, the United States, and the European Union

The process whereby cyberspace regulation is formulated in Israel consists of two major stages, but they too, as noted, lack a national strategy for all market sectors.[45] Israel's cyberspace regime started in 1998 with the law regulating security in public institutions. The law listed all the requirements for protecting information systems of institutions defined as "critical" to the state. These included aerospace, water, electricity, and communications bodies. In 2002, the state determined that the professional supervisor for these institutions would be the National Information Security Authority, which is subordinate to the Israel Security Agency (Shin Bet).[46] Furthermore, the

state determined that the institutions receiving directives from the National Information Security Authority would be carefully selected by a special steering committee; in practice, the list of bodies swelled with the passage of time. In other words, bodies defined as critical to the state, based on the impact of the potential damage (for the GDP, for example), received a state-mandated directive, whereas many other bodies, which were not defined as having the potential for great damage, were left without guidelines, thus leading to a situation in which the economic considerations of the market forces became the major factor in their defense. It should be noted that the institutions receiving directives include both private and public ones (oil refineries, El Al, the Israeli Electric Corporation, Israel Railways, and so forth).

In 2011, Israel entered the second stage of its development of cyberspace regulation when the government changed its approach and started to address the work required with the private sector. The National Cyber Bureau (NCB) was established under the Prime Minister's Office, a move designed to create better integration with market actors. Later, in 2015, the National Cyber Authority was founded with the objective to work directly with the civic sector and serve as the executive body for the state's cyber defense efforts. The Israeli regulatory state in cyberspace can be described schematically as follows:

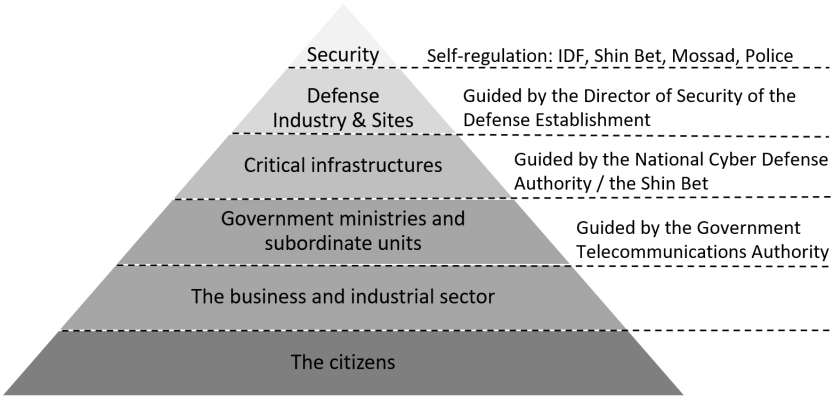

Figure 2: State regulation of cyberspace in Israel

The chart above particularly highlights two aspects. As previously noted, the civic sector is mostly left unsupervised. Although there are little islands

of supervision—the financial, energy, and healthcare sectors—guided by directives from government units, themselves subject to the guidelines of the Government Information and Communication Technology (ICT) Authority. But by and large, the civic sector engages in self-regulation, lacks information sharing, and mitigates data breaches to its customers as it sees fit.

Other than its selective supervision of different sectors, Israel recently issued two significant policy guidelines. The first, designed to enhance supervision already carried out by the Defense Exports Supervision Division at the Defense Ministry, expanded the list of products requiring state supervision, reflecting the state's desire to supervise the cyberspace arms race and maintain Israel's relative advantage.[47] The state has decided to halt this process and continue consulting with the cyber industry about the issue and, for now, adhere only to international supervisory arrangements, given the opposition from the local industry that was concerned it would not be able to compete with industries in unsupervised states.[48] The desire to maintain Israel's standing in the world as a leading cyberspace exporter relative to its population[49] resulted in the preservation of the status quo in the issue of supervision. This is instructive regarding the depth of the mutual understanding and extensive cooperation between the various industries and the Defense Ministry.[50] The ministry listened to the concerns of the industry, managed to get a toehold, and is now part of the decision-making process for every cyberspace product designed for attack.

The objective of the second guideline is to nurture human capital and create standards for those defending cyberspace. This is an entry regulation, based on official recommendation, in which the state delineates the professional level required of personnel in all forms of cyber defense.[51] This is a significant guideline, which has not been tried extensively elsewhere in the world. It may, on the one hand, raise the professional level on the short term through various training programs that could be developed especially for regularization; yet, on the other hand, this guideline could obviate the self-taught model by which most experts in this dynamic field currently attain their knowledge.[52]

Cyberspace Regulation in the Civic Sector: Importance and Difficulties

Despite the wide range of efforts described herein, the civic sector in Israel is not subjected to cyberspace regulation and its security lacks state

supervision.[53] This challenge traverses national borders, as manifested both in the United States and the European Union (until the two most recent European Union directives, which for the first time also cover industries in the civic sector). When it comes to the resilience of the shared cyberspace, it is difficult to overstate the importance of the civic sector. First, the civic sector represents the lion's share of the sphere. It is exposed to most of the threats and is traditionally the weakest link through which attacks begin and spread to other sectors. Second, private companies regularly provide services to government ministries and sensitive state institutions, making their resilience in cyberspace a primary concern. Third, damage to the private sector is damage to the stability of the entire economy. Under certain conditions, this could significantly harm the nation's resilience. The policy of expanded privatization has only exacerbated the problem, making the private sector the key player in the state's regulatory efforts. Fourth, the civic sector is responsible for technological developments upon which more sensitive sectors rely; thus, damage to it could serve as a backdoor to attacks on sensitive information.[54] This is especially true for startups poor in defensive resources, but that sometimes end up developing defense products for general use.[55]

The private sector's basic opposition to regulation is not surprising and is a familiar phenomenon in other contexts as well. State regulation and supervision are seen as hamstringing commercial companies and costing them a great deal in return for little value.[56] Moreover, the private sector considers the state to be slow to react to technological change and incapable of meeting the inherent challenges in supervising a dynamic, constantly changing technological sphere.[57] Instead of increasing the resilience of commercial companies, state regulation might force them to adopt standards that do not match current threats and take away the flexibility they enjoy today. Finally, the idea of state intervention is inconsistent with the neo-liberal approach that has spread like wildfire in twentieth century's capitalist societies,[58] where the regnant paradigm is one of privatization and deregulation, whereby the state intervenes only minimally, if at all, in the market to maximize the benefits accrued by commercial entities.[59]

Concluding Insights

Although Israel is developing its National Cyber Authority, many economic sectors still lack guidelines and supervision that would ensure appropriate protection. There is no road map to ensure the resilience of the civic sector and to serve as a model to be adopted by the different players in the economy. Such a model would have to address several key issues:

First, the model would have to generate a structured process that would provide civilian bodies with the incentive to adopt cybersecurity. Entry regulation, such as a local government business licensing law, is one way, but other options also may be considered. The state is currently working on a "cyber law" that aims to create a kind of cybersecurity verification seal that would define a uniform defense standard necessary to market companies.[60] The need for such a security seal might incentivize institutions to protect themselves better.

Second, it is necessary to consider the various layers of the civic sector. There is no one-size-fits-all solution; rather, it is crucial that the regulation be tailored to the type of enterprise, its level of information sensitivity, manufacturing processes, and supply chains of the various companies on the market. Therefore, it is necessary to rank the civic sector by its exposure to risk and the damage that a systems breach is liable to cause; an insurance company, for example, cannot be treated the same as a pharmaceutical manufacturer. The proposed model would have to address these essential differences.

Third, it is necessary to consider expanding the risk strategies the state is using. The lateral look at Israeli regulation in this essay teaches us that the state is primarily involved in preventing cyber risks from being realized. Mechanisms now emerging in the United States[61] to encourage information sharing—with the built-in tension over safeguarding the right to privacy—might make it possible to relieve the bottleneck of information sharing and create a more effective, proactive cybersecurity. In addition, it is necessary to enhance transparency over data breaches by requiring all sectors to notify a national CERT and share information with the public. This will help others understand where caution is needed and the extent to which sensitive information is at risk. These could serve as incentives for better defense and more effective damage mitigation. Commercial companies that worry about

having to pay for damage mitigation by law will defend themselves ahead of time as best they can.

To conclude, the need for regulating cyberspace in the civic sector is obvious, but the difficulties of developing such regulation are numerous; they range from the problems and battles between state institutions, the tensions between competing interests, the costs involved in adhering to regulation, and the attempts to find the right balance between transparency and secrecy as well as between centralization and decentralization. At present, even though cyberspace is essentially a civic sphere—most of it being based on civilian infrastructures, systems, and technologies operated by civilian organizations—this sector has not yet been regulated and incorporated into Israel's regulatory regime. The responsibility for cybersecurity currently rests on the organizations alone, even though the lone organization lacks the expertise and resources to confront cyber threats without creating an infrastructure for cooperation between the various sectors in the economy. Israel is quite active in the state's cyberspace as cyber units were established in the Prime Minister's Office, the decision to establish a cyber force was made, and various R&D settings and national research centers were founded. Nonetheless, it is incumbent upon the state to continue to strive to strengthen the defense of the relevant civic sectors using a range of tools and capabilities, because damage to the civic sector is liable to cause fundamental harm to the entire nation.

Notes

1 The resilience of cyberspace refers to the sphere's ability to withstand possible attacks aimed at software and hardware weaknesses, non-secure protocols, and unauthorized information access.

2 The development of these protocols met the needs at the beginning of the worldwide web in the 1960s. In those days, it was necessary to allow connectivity among just a few dozen computers. At the time, nobody predicted that a web consisting of billions of users would be using the same protocols.

3 Zero-day weaknesses are hardware or software weaknesses, generally unknown to the manufacturer, that have yet to be fixed. Sometimes they are known weaknesses for which patches have not yet been issued to all relevant systems. About this flourishing market, see Andy Greenberg, "New Dark-Web Market is Selling Zero-Day Exploits to Hackers," Wired.com, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits.

4 Internal documents of an Italian company, Hacking Team, recently were exposed, showing the company trafficked in weaknesses and the development

of attack tools. The documents showed the company's commercial ties with various regimes around the world. For more on the phenomenon, see Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," *New York Times*, May 29, 2016, http://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?ref=topics&_r=0.

5 Jason and Peter, "Cyber Security: A critical examination of information sharing versus data sensitivity issues for organizations at risk of cyber attack," *Journal of Business Continuity & Emergency Planning* 7, no. 2 (2014):10–111.

6 Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy*, Memorandum 153 (Tel Aviv: The Institute for National Security Studies, 2016) http://www.inss.org.il/uploadImages/systemFiles/INSS%20Memorandum%20153%20-%20Guidelines%20for%20a%20National%20Cyber%20Strategy.pdf.

7 Bruce Schneier, "Credential Stealing as an Attack Vector," Xconomy.com, April 20, 2016, http://www.xconomy.com/boston/2016/04/20/credential-stealing-as-attack-vector/.

8 Nate Lord, "The History of Data Breaches," digitialguardian.com, September 28, 2015, https://digitalguardian.com/blog/history-data-breaches.

9 Ulrich Beck, *Risikogesellschaft: auf dem Weg in eine andere Moderne* (Frankfurt am Main: Suhrkamp, 1986). The book appeared in English as *Risk Society: Towards a New Modernity* (London: Sage,1992).

10 David Moss, *When All Else Fails: Government as the Ultimate Risk Manage* (Cambridge: Harvard University Press, 2002).

11 Ibid.

12 See the full defense circle in Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affair*s, May 7, 2015.

13 Third-party risks in cyberspace are the risks to the privacy of customers of commercial companies damaged by cyberattacks and by the theft of personal information. On the other hand, insurance companies are less than thrilled to ensure first-party risks because there is a lack of actuarial data that would help them price the insurance premiums for cyberspace risks of the companies themselves (i.e., first-party risks).

14 David Levi-Faur, "Regulation: Conceptual and Historical Background," (University of Haifa, no date), (in Hebrew). See also, David Levi-Faur "The Odyssey of the Regulatory State," *Jerusalem Papers in Regulation & Governance*, Working Paper no. 39 (November 2011), http://regulation.huji.ac.il/papers/jp39.pdf.

15 Ibid.

16 Ibid.

17 A state that mainly regulates for efficiency purposes, through laws, rather than investments and subsidies. See Giandomenico Majone, "The Rise of The Regulatory State in Europe," *West European Politic*s 17, no. 3 (1994): 77–101, http://dx.doi.org/10.1080/01402389408425031.

18 In his essay "Regulation and Regulatory Governance," Levi-Faur explains why deregulation obviates the formation of more agencies and the hiring of more bureaucrats to supervise privatization processes and guard the state's interests while it also accelerates the process. See David Levi-Faur, "Regulation and Regulatory Governance," *Jerusalem Papers in Regulation & Governance*, Working Paper no. 1 (February 2010), http://levifaur.wiki.huji.ac.il/images/Reg.pdf.

19 Ibid.

20 Shurik Dryshpitz, "Regulation: What, Where, and When? A Theoretical and Comparative Perspective" in "Who Privatized My State? Privatization, Regulation, and the Third Sector: Theory and Practice," *Parliament* 64 (Jerusalem: The Israel Democracy Institute, 2012), (in Hebrew), http://www.idi.org.il/parliaments/64/11149.

21 See, for example, Harold Demsetz, "Why Regulate Utilities?" *Journal of Law and Economics* 11 (1968): 55–65.

22 For an empirical research on the actions of interest groups in the United States, see Frank R. Baumgartner and Beth L. Leech, "Interest Niches and Policy Bandwagons: Patterns of Interest Group Involvement in National Politics," *Journal of Politics* 63 (2001):1191–1213.

23 On the way that policy networks to protect privacy in Europe created stronger institutions, which passed more rigid privacy laws contrary to the spirit of the time, see Abraham L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive," *International Organization* 62, no. 1 (2008): 103–130.

24 On the consistency of the modern welfare state, see Paul Pierson, ed. *The New Politics of the Welfare State* (Oxford: Polity Press, 2001).

25 On shattering the Keynesian paradigm and transitioning to a monetary economy in the United Kingdom, see Peter Hall, "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain," *Comparative Politics* 25, no. 3 (1993): 27–296.

26 John Kingdon's study coined phrases such as "window of opportunity" and "policy entrepreneur," which explain—with astonishing accuracy—public policy procedures. See John W. Kingdon, *Agendas, Alternatives, and Public Policy*, 2nd edition (Boston, Little Brown, 1995).

27 Daniel Béland and Robert Henry Cox, eds. *Ideas and Politics in Social Science Research* (Oxford: Oxford University Press, 2010).

28 While the European Union differs from the classical state institution, it is still a seminal object for comparative research in the field. Decisions at the EU level led to a rigid information security policy through the European Union (see Newman 2008 and below), and the directives formulated at the EU level led the way for the individual states. This is valid not only for the world of cyberspace, but also can also be observed in contexts of food safety regulation and the introduction of genetically engineered food throughout the continent. For the importance of EU regulation, see David Bach and Abraham L. Newman, "The European Regulatory

State and Global Public Policy," *Journal of European Public Policy* 14 no. 6 (2007): 827–846.

29 Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security," *Georgetown Journal of International Affairs*, International Engagement on Cyber, IV, (2014): 69–78.

30 For the ways in which hackers share information in the darknet, see the interview with Stuart Madnick from MIT in Linda Tucci, "Stuart Madnick: Dark Web hackers trump good guys in sharing information," techtarget.com, April 30, 2016, http://searchcio.techtarget.com/news/450295259/Stuart-Madnick-Dark-Web-hackers-trump-good-guys-in-sharing-information.

31 Increased government intervention and centralization.

32 See the thought-provoking philosophical debate over the terms "zero-sum game" and "necessary balance" between security and individual liberty in Jeremy Waldron, "Security and Liberty: The Image of Balance," *Journal of Political Philosophy* 11, no. 2 (2003): 191–211.

33 These methods to confront the risks come up in the examination of how regulation has been put in place over the years in the United States (at the federal and state levels) and in the European Union (at the EU level and individual state levels).

34 For example, US courts recently gave the Federal Trade Commission the authority to enforce information protection laws in the private sector. For more information, see Brent Kendel, "Appeals Court Affirms FTC Authority Over Corporate Data-Security Practices," *Wall Street Journal*, August 24, 2015, http://www.wsj.com/articles/appeals-court-affirms-ftc-authority-over-corporate-data-security-practices-1440425754.

35 The abbreviation stands for Cyber Emergency Readiness Team, a regulatory agency now in existence in virtually every state. It collects data on all cyberbreaches requiring notification and integrates responses to significant events happening in cyberspace.

36 Gabi Siboni, May 7, 2015.

37 For example, guidelines issued by the Information Security Authority in Israel about the way to secure organizational networks.

38 For an explanation of ISO standards at the official website, see http://www.iso27001security.com/html/27032.html.

39 For an explanation of PCI standards at the official website, see https://www.pcisecuritystandards.org/.

40 See, for example, the standards the organization issued: http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

41 For example, the latest FINRA report issued on the topic: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

42 Richard J. Harknett and James A. Stever, "The New Policy World of Cybersecurity," *Public Administration Review* (2011): 455–460.

43 For details, see National Conference of State Legislators (NCSL), Security Breach Notification Laws, April 1, 2016, http://www.ncsl.org/research/

telecommunications-and-information-technology/security-breach-notification-laws.aspx.

44 For details on the effect of European regulation on the security level of commercial companies, see Ashford Warwick, "Breach Notification the Biggest Impact of EU Datalaw Overhaul, Says Law Firm," computerweekly.com, November 27, 2015, http://www.computerweekly.com/news/4500258249/Breach-notification-the-biggest-impact-of-EU-data-law-overhaul-says-law-firm.

45 Siboni and Assaf, *Guidelines for a National Cyber Strategy*.

46 In 2015, the National Cyber Defense Authority was established, assuming responsibility of most of Israel's critical infrastructure.

47 The expansion applies primarily to penetration products, hacking analysis, and knowledge of software and hardware weaknesses.

48 For more information, see article by guest writer, "What Lay Behind the Repeal of the New Cyber Injunction," *Geektime*, April 2016, (in Hebrew), http://www.geektime.co.il/the-decline-of-the-israeli-cyber-law/.

49 For the change in the southern city of Beer Sheba, which the state decided to recreate as the region's cyberspace export capital, see Ashford Warwick, "Israel's cyber security frontier," computerweekly.com, May 2016, http://www.computerweekly.com/opinion/Israels-cyber-security-frontier.

50 See Wexman and Hindin, "How Does Israel Regulate Encryption?" lawfareblog.com, November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption.

51 For the official regularization document, see Prime Minister's Office, National Cyber Staff, "Profession Regulation Policy for Cyberdefense in Israel," December 31, 2015, (in Hebrew), http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf.

52 See report on the subject, National Academy of Science, "Professionalizing the Nation's Cybersecurity Workforce," 2013, http://www.nap.edu/catalog/18446/professionalizing-the-nations-cybersecurity-workforce-criteria-for-decision-making.

53 This is with the exception of specific entities, such as the banks, and the privacy law, which applies to the entire economy, although it is not sufficiently up-to-date in terms of all aspects of information security. For a survey of the situation, see Raphael Kahan, "Netanyahu markets Israeli cyber but legislation is full of holes," *Calcalist*, June 2015, (in Hebrew), http://www.calcalist.co.il/internet/articles/0,7340,L-3662815,00.html.

54 For a more in-depth survey of some of these reasons, see Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security," *Georgetown Journal of International Affairs,* International Engagement on Cyber, IV, (2014):69–78.

55 Gabi Siboni and David Israel, "Cyberspace Espionage and Its Effect on Commercial Considerations," *Military and Strategic Affairs* 7, no. 3 (December 2015): 39–58, http://www.inss.org.il/uploadImages/systemFiles/INSS.MASA-7.3-Full(ENG).pdf.

56 Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security."

57 Ibid.

58 For a survey of the neo-liberal trend in capitalist societies, see John Dryzek, *Democracy in Capitalist Times: Ideas, Limits, and Struggles* (Oxford University Press, 1996).

59 Does privatization really lead to deregulation? For a challenge to the justifications for privatization, see Yitzhak Gal-Noor, "The Policy of Privatization: Whose Burden of Proof Is It?" (Jerusalem: Hebrew University and the Van Leer Institute, 2014), (in Hebrew). For regulation in the privatization era, see David Levi-Faur, Noam Gidron, and Smadar Moshel, "The Regulatory Deficit of the Privatization Era," (Jerusalem: Van Leer Institute, 2014), (in Hebrew).

60 See Yossi Melman, "Closed code: State promoting cyber defense law in light of increased attacks," *Maariv*, February 2016, (in Hebrew), http://www.maariv.co.il/journalists/Article-524985.

61 See Andy Greenberg, "Congress Slips CISA into a budget bill that's sure to pass," Wired.com, December 16, 2015, http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/; Tim Greene "CISA Legislation would fit liability for businesses sharing cyber threat information," networkworld.com, October 28, 2015, http://www.networkworld.com/article/2998815/security/cisa-legislation-would-lift-liability-for-businesses-sharing-cyber-threat-information.html.

Artificial Intelligence in Cybersecurity

Nadine Wirkuttis and Hadas Klein

Cybersecurity arguably is the discipline that could benefit most from the introduction of artificial intelligence (AI). Where conventional security systems might be slow and insufficient, artificial intelligence techniques can improve their overall security performance and provide better protection from an increasing number of sophisticated cyber threats. Beside the great opportunities attributed to AI within cybersecurity, its use has justified risks and concerns. To further increase the maturity of cybersecurity, a holistic view of organizations' cyber environment is required in which AI is combined with human insight, since neither people nor AI alone has proven overall success in this sphere. Thus, socially responsible use of AI techniques will be essential to further mitigate related risks and concerns.

Keywords: cybersecurity, artificial intelligence (AI), security intelligence, Integrated Security Approach (ISA), cyber kill chain

Introduction

Since 1988, when the first denial-of-service (DoS) attack was launched,[1] the sophistication, number, and impact of cyberattacks have increased significantly. As cyberattacks have become more targeted and powerful so have cybersecurity countermeasures. While the first security tool was limited to spotting signatures of viruses and preventing their execution, today we find solutions that are designed to provide holistic protection against a wide range

Nadine Wirkuttis is a PhD candidate at the Okinawa Institute of Science and Technology Graduate University and former research intern in the Cyber Security Program at the Institute for National Security Studies. Hadas Klein is the Cyber Security Program Manager at the Institute for National Security Studies.

of attack types and a variety of target systems; nevertheless, it has become increasingly challenging to protect information assets in the virtual world.

To implement resilient and continuous protection, security systems need to constantly adjust to changing environments, threats, and actors involved in the cyber play. Cyber reality, however, appears somewhat different. Security approaches are regularly tailored to known attacks, and due to a lack of flexibility and robustness, security systems typically are unable to adapt automatically to changes in their surroundings. Even with human interaction, adaption processes are likely to be slow and insufficient.[2]

Due to their flexible and adaptable system behavior, artificial intelligence (AI) techniques can help overcome various shortcomings of today's cybersecurity tools.[3] Although AI has already greatly improved cybersecurity,[4] there are also serious concerns. Some view AI as an emerging existential risk for humanity.[5] Accordingly, scientists and legal experts have expressed alarm at the increasing role that autonomous AI entities are playing in cyberspace and have raised concerns about their ethical justifiability.[6]

The purpose of this work is to highlight the shortcomings of traditional security measures as well as the progress that has been made so far by applying AI techniques to cybersecurity. In addition, this work summarizes the risks and concerns linked to this development, by exploring AI's status quo, addressing present concerns, and outlining directions for the future.

Challenges of Today's Cybersecurity

Although awareness of cyber threats has increased; large amounts of money has been invested; and efforts are being made to fight cybercrimes, the ability of organizations to sufficiently protect their own virtual assets is not yet known.[7] The involved parties in cyberspace range from single individuals, private organizations, non-state actors to governmental organizations, all aiming to protect their cyber assets, attack those of others, or both. In addition, the sources of cyber threats are manifold: cyber threats basically arise from potential malicious acts due to financial, political, or military reasons.[8]

However heterogeneous and dynamic the nature of cyberspace might be, certain similarities of attacks and their countermeasures can be used to describe and allow for a holistic security framework. Most cyberattacks follow certain attack phases that can be described as a **cyber kill chain**.[9] This framework assumes that every attack sequence starts with a **reconnaissance** phase**,** in

which an attacker tries to locate gaps and vulnerabilities of a target system. The **weaponizing** phase follows, during which the uncovered weaknesses are used to develop targeted malicious code. This is followed by the **delivery** phase when the malware is transferred to the potential target. After the malware is delivered successfully, the **exploit** phase occurs during which the malware triggers the installation of an intruder's code. Afterwards, the compromised host system allows the establishment of a command and control channel so that the attacker can initiate malicious actions. Counteractions can be determined depending upon where a malicious action appears in the cyber kill chain.

The **integrated security approach**[10] (ISA) provides key ideas for a holistic view on cyber defense and a framework for such categorization. The main aim of the ISA is to generate **early warnings**, or alarms, preferably before the attack is launched (before the exploit phase**)**. The alarm is supposed to generate a relevant warning message that translates newly gathered threat data into actionable tasks. By this means, the message further supports the selection of countermeasures or already contains dedicated counteractions to prevent organizations from being victims of an attack. If an intrusion can not be prevented in advance, the extent of the attack must be detected, followed respectively by reaction and response. These measures should include actions to stop or counterattack the invader, in addition to defining recovery procedures to quickly rollback the system to its initial state.

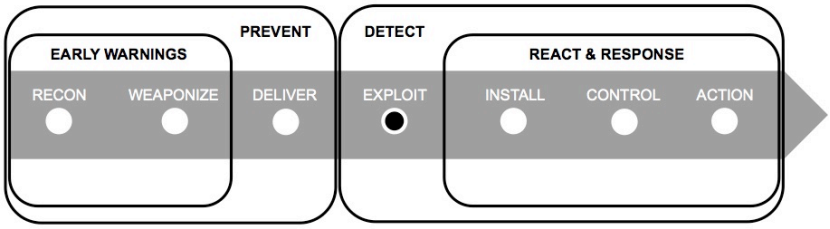

Figure 1: Cyber kill chain phases encapsulated in countermeasures of the integrated security approach

Figure 1 above depicts the interconnection of cyberattacks, described by the cyber kill chain, with their countermeasures, covered by the ISA. The diagram depicts the cyber kill chain, here visualized as the gray arrow in the center, encapsulated by the ISA. The cyber kill chain includes the seven

phases of a cyberattack, whereas the ISA consists of four counteraction phases. For detecting and blocking attacks as early as possible, all attack phases of the cyber kill chain need to be considered within the comprehensive ISA framework.[11] As stated above, the emphasis is on preventing attack and detecting malicious activities during the first three phases of an intrusion, here visualized as recon, weaponize, and deliver on the left side of the diagram within the gray arrow. After the attack—depicted as exploit in the center of the arrow—the ISA measures detection, reaction, and response necessary to interfere with the compromising malicious activities.

The complex and dynamic nature of cyberspace leads to various strategic and technological challenges that hinder and complicate an organization's ability to protect itself sufficiently in this virtual environment. These challenges comprise data acquisition, technology driven matters, as well as shortcomings in regulation and process management.

Challenges in Gathering Cyber Intelligence

The fact that perpetrators leave tracks when attempting to attack a potential target system is the key to better understanding an attacker. Consequently, an ISA with its holistic view of an organization's security requires gathering and analysis of a range of information for gaining cyber intelligence.[12] There are challenges, however, in acquiring relevant data as well as in processing, analyzing, and using it. Therefore, related efforts to effectively prevent, detect, and respond to malicious intrusions are regularly aided by security tools that aim to automate supporting security processes. The main **challenges in acquiring relevant data tracks** are:[13]

a. Amount of data: The amount of data has increased exponentially since electronic devices and their use has become ubiquitous in our work and daily lives. For the implementation of an ISA, data from all systems across entire organizations may need to be considered.
b. Heterogeneity of data and their sources: The variance in data and its sources makes it difficult to identify and collect those data; moreover, both are spread across organizational and national borders. Even if the relevant heterogeneity within the cyber environment is identified, topology and behavior of systems and networks may change and, thus, require constant adaption.

c. High data velocity: The high rate at which data is produced and processed within its sources leads to challenges in data storing and processing, which, in turn, is essential for subsequent analysis.

When it comes to processing, analyzing, and using the acquired date, **intrusion detection prevention systems** (IDPS) have proved to be an invaluable tool for cybersecurity,[14] one of many in today's cybersecurity arsenal. An IDPS is either software or hardware configured to protect single systems or entire networks. There are two main principles for IDPSs: the **misuse detection** approach, which identifies malicious activities by defining patterns of abnormal network and/or system behavior, and the **anomaly detection** approach, which is based on defining patterns of normal network and/or system behavior. Security experts define both patterns, mainly based on their experiences plus their prior knowledge of cyber threats.[15]

Cyber reality, however, is a highly complex and dynamic nature; new threats appear constantly, and attacks are specifically tailored to circumvent known protection scenarios. While the desired characteristics of IDPSs are optimized performance, maximum protection, and minimum error,[16] traditional security systems are no longer able to fully fulfill these requirements. The most **critical technological weaknesses** are:[17]

a. Low detection rate: Any inaccuracy in defining patterns of abnormal or normal network and/or system behavior may affect the IDPS's detection rate. The continuously changing network environment makes this task even more challenging. Errors in defining abnormal patterns can lead to high false negative detection rates. Here, the malicious network activities of attempted attacks are not detected in advance because a non-malicious network behavior was assumed instead. By contrast, erroneous definition of normal patterns can cause high false positive rates, causing non-malicious network activities to be categorized as malicious.
b. Slow throughput: IDPSs can show limitations in processing and analyzing gigabits of data per second. Mechanisms that address this issue are based mainly on the distribution of data processing and, thus, can further affect the system's operation, maintenance, and related costs.
c. Lack of scalability and resilience: Cyber environments are dynamic. Infrastructures and network traffic change and expand constantly, and vast amounts of heterogeneous data needs to be processed and analyzed. These dynamics further lead to performance issues and a loss of efficiency,

as IDPSs might be not able to provide and maintain their functionalities when coping with these dynamics.

d. Lack of automation: IDPSs are not yet able to adapt automatically to changes in their environment. This can result in the need for individual analysis of log data; the manual readjustment of systems to changes in the network environment; or for experts to determine the appropriate reaction for every individual warning message. This lack of automation results in a constant need for human supervision, and causes delays as well as an overhead in costs and resources.

Due to the technological challenges, organizations may face security deficits at some point; they may use several security systems or purchase security intelligence, in terms of security consulting, through third-party providers.[18]

Additional Challenges

Besides the comprehensive acquisition of data and the use of solid security technologies for protecting the full range of information in a timely manner, supporting processes also need to be considered. The establishment and maintenance of these processes is as important as data acquisition and the use of appropriate security technologies. Inter-organizational as well as intra-organizational processes can help to further improve and maintain organizations' ISAs, in addition to increasing their cybersecurity maturity level.[19] Furthermore, the creation of a so-called **cyber ecosystem**[20] encourages partnerships between diverse actors across the cyber landscape that aim to address and share security threats, experience, or resources.

Organizations operating in different sectors also tend to have inconsistent demands of cybersecurity. These differences can correspond to heterogeneous security requirements as well as varying responses when facing similar cyberattacks.[21] In cases where organizations need to protect critical infrastructures, such as water treatment or nuclear power plants, they focus on increased security rather than on financial aspects. In comparison, private organizations tend to focus on financial losses and do not give too much importance to endangering public safety.[22]

These are only some of the challenges that trouble organizations when setting up their security strategy. Given the important role of security systems in this context, the following section will focus on the technological measures.

Intelligent Techniques to Facilitate Security Measures

In tackling intelligence-gathering issues for cybersecurity, intelligent machines show promise of improving today's security measures. Intelligent machines can perform some human cognitive abilities (ability to learn or reason) as well as having sensory functions (ability to hear or see). These machines exhibit what we could call **intelligence**.[23] Such artificial intelligence enables machines to behave intelligently and imitate human intelligence—albeit to a limited extent.

The development of intelligent systems, either software or hardware, provides methods to solve complex problems—problems that could not be solved without applying some intelligence.[24] Whereas traditional computer systems are based on fixed algorithms[25] and require known data formats for decision making, the computer science discipline of AI developed flexible techniques, such as the recently revived approach of deep neural networks, that enables machines to learn[26] and adapt automatically to the dynamics of their environment. In cyberspace, this may include the automatic adaption to heterogeneous data formats, changing data sources, or noise[27] in cyber activities.

In the realm of AI, cybersecurity arguably is the industry that could benefit most from the introduction of machine intelligence; furthermore, the challenges of conventional security systems are supposed to be overcome by using autonomous AI systems.[28] Consequently, the issues in data acquisition (amount, heterogeneity, and velocity of data) as well as the problems of the related tools (low detection rate, slow throughput, a lack of scalability and resilience, and a lack of automation) could be mitigated through AI. Thus, efficiency and the effectiveness of cybersecurity and its respective tools could be improved.

The field of AI has developed and is still developing numerous techniques to address intelligent system behavior, and many have been established already in the field of cybersecurity. These systems can therefore handle and analyze vast amounts of information within a reasonable time frame and in the event of an attempted attack, can analyze the information and select dedicated counteractions. Possible scenarios, where AI techniques are applied to security issues related to the four categories within the ISA, can demonstrate the vast possibilities of the various branches of AI.

Interacting Intelligent Cyber Police Agents to Monitor Entire Networks

The paradigm of **intelligent agents** is a branch of AI that arose from the idea that knowledge in general and, especially, knowledge to solve problems ought to be shared between different entities. A single agent is an autonomous cognitive entity,[29] with its own internal decision-making system and an individual goal. To achieve its goal, an agent acts proactively within its environment and with other agents. In addition, agents have a reactive behavior; they understand and respond to changes in their environment and interact with it and other decentralized agents. Over time, agents self-adapt to dynamic changes in their environments, given their own accumulated experiences.[30]

Due to their decentralized and interacting nature, intelligent agents are predestined to gather information on entire networks and surrounding systems. It appears that this favorable characteristic has been used not only in terms of defense measures, but also for reconnaissance and exploitation (see the cyber kill chain discussed above) of potential target systems.[31] Since the behavior of every agent is formed by its experiences within its own personal environment, it is quite challenging to protect against such individualized threats.

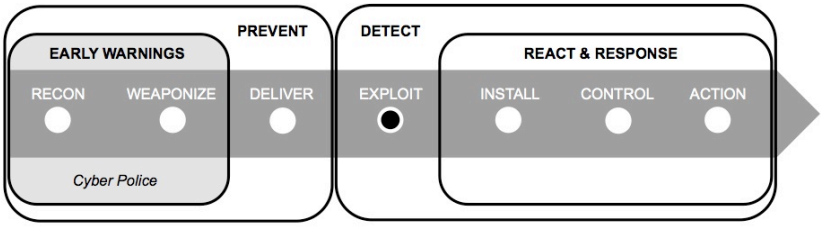

Figure 2: Intelligent Cyber Police Agents for Early Warnings in an Integrated Security Approach

A powerful way to utilize agents against distributed cyberattacks is by building up an intelligent agent's cyber police. This approach pursues the idea of artificial **police agents** in a defined cyber environment to detect malicious activities in a decentralized way.[32] As visualized in Figure 2 above, such police agents can facilitate protection already in the earliest stages of a cyberattack.

Intelligent agents can also be found in human-inspired artificial immune systems (AISs). By using two different types of agents, detection and counterattack agents, the beneficial characteristics of the human immune system is imitated. Detection agents monitor cyber environments and try to detect abnormal activities. When these agents spot malicious activities, they proactively send out decentralized instructions to counterattack agents, which are then activated to prevent, mitigate or even counterattack network intruders.[33]

Artificial Neural Networks to Prevent Malicious Intrusions

Another technique that emerged from the field of AI is the **artificial neural network** (ANN). ANNs are statistical learning models imitating the structure and the function of the human brain. They can help to learn and solve problems, especially in environments where algorithms or rules for solving a problem are difficult to express or are unknown. Since ANNs' system behavior is kind of elusive, they are considered undefined black-box models.[34]

In cybersecurity, ANNs have been used successfully within all stages of ISAs and, hence, can encapsulate all phases of the cyber kill chain. Integrated in cybersecurity, ANNs can be used for monitoring network traffic. As depicted in Figure 3 below, malicious intrusions can be detected already during the delivery phase and before an actual attack occurs.[35] This is a desired goal of cybersecurity, and it is a great achievement when cyberattacks can be hindered before they take place, thus, elaborating upon the main idea of perimeter defense.[36] ANNs can be successfully used to learn from past network activities and attacks in order to prevent future attacks from actually transpiring.

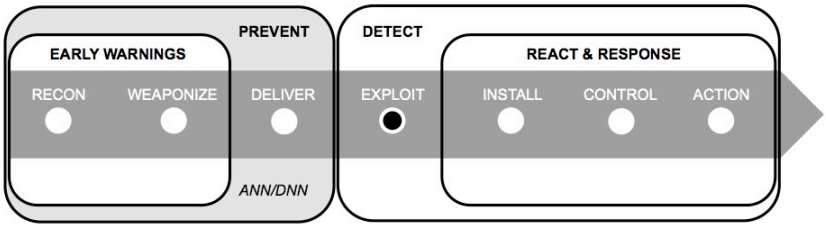

Figure 3: Artificial Neural Networks to Prevent Attacks within an Integrated Security Approach

Compared to conventional techniques used for cyber defense, the great advantage of using ANNs is their learning ability. As mentioned above, patterns that describe normal and abnormal network activities are traditionally defined manually by security professionals based on their expert knowledge. ANNs, however, can be trained to identify such patterns automatically by using previous data that has been transferred over the network.

Within an anomaly-based IDPS approach, it was shown that ANNs can be successfully utilized to evaluate header information[37] of network data packages to *learn* patterns for normal network behavior.[38] In a first preparatory step, the ANN was trained to identify and learn patterns of header attributes that belonged to normal network traffic. Every future data packet that was transferred over the monitored network was compared afterwards with these pre-learned patterns. When attributes of packet headers matched the *normal* pattern, they were transferred as usual. Irregularities in a data packet's header information that mismatched the learned pattern were classified as malicious and rejected by the IDPS. This dedicated approach has shown that the overall detection rate of attempted intrusions has improved without generating any false positive or false negative alarms. While traditional IDPSs, both signature-based and anomaly-based, work mostly against known intrusions, this ANN approach has successfully protected against instances of intrusions that were previously unknown. In summary, ANNs are said to support a viable approach to building robust, adaptable, and accurate IDPS.[39]

ANN monitoring is not limited to the use within IDPSs; it can be established in every system that monitors network activities. Firewalls, intrusion detection systems, or network hubs use ANNs to scan incoming as well as outgoing network traffic. In malware detection, an ANN-based experimental simulation demonstrated that even with quite a small computational effort, 90 percent of malware could be detected in advance.[40]

Deep neural networks (DNN), a more elaborate and computationally expensive form of ANNs,[41] have been used recently not only to protect organizations from cyberattacks, but also to predict these attacks. Improvements in hardware have led to advancements in data processing within network infrastructures and have enhanced storage capacities; thus, DNN technologies have become more popular and applicable. A dedicated AI-based security platform that used a DNN approach successfully demonstrated that it could predict cyberattacks 85 percent of the time.[42] With this development, we

see traditional approaches of cybersecurity shifting from attack detection to attack prevention. DNN techniques can now possibly lead in a new phase of cybersecurity—namely cyberattack prediction.

Expert Systems to Provide Decision Support for Security Professionals

Expert systems are computer programs designed to provide decision support for complex problems in a domain; these are the most widely used AI application. Conceptually, an expert system consists of a knowledge base, which stores the expert knowledge, and an inference engine, which is used for reasoning about predefined knowledge as well as finding answers to given problems.[43]

Depending on the way of reasoning, expert systems apply to different problem classes. A case-based reasoning (CBR) approach allows solving problems by recalling previous similar cases, assuming the solution of a past case can be adapted and applied to a new problem case. Subsequently, newly proposed solutions are evaluated and, if necessary, revised, thus leading to continual improvements of accuracy and ability to learn new problems over time. Rule-based systems (RBS) solve problems using rules defined by experts. Rules consist of two parts: a condition and an action. Problems are analyzed stepwise: first, the condition is evaluated and then the action that should be taken next is determined. Unlike CBR systems, RBSs are not able to learn new rules or automatically modify existing rules. This fact refers to the "knowledge acquisition problem," which is crucial in adapting to dynamic environments.[44]

Security professionals widely use expert systems for decision support in cyber environments. In general, evaluating security systems' audit data can determine whether a network or system activity is malicious or not. Due to the large amount of data, security experts regularly use statistical reports to scan and analyze the whole audit information in a reasonable time span. AI-based expert systems have successfully demonstrated that they could support these efforts by performing real-time monitoring in cyber environments, even on numerous or heterogeneous systems.[45] In cases where a malicious intrusion was spotted, a warning message was generated. It provided relevant information, upon which security professionals could select appropriate security measures more efficiently (cf. react & respond in Figure 4 below).

At this point, it is crucial to recall that expert systems so far solely assist decision makers, but are not able to substitute for them.[46]

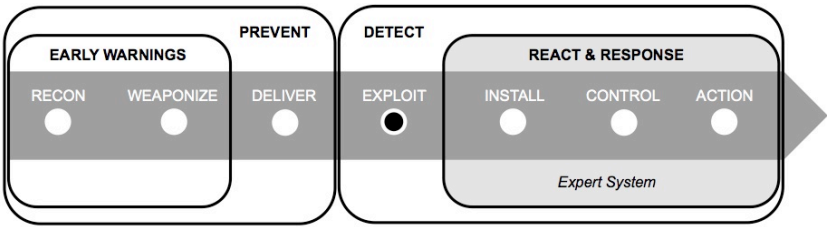

Figure 4: Expert Systems to Support React & Response Measures in an Integrated Security Approach

Drawbacks of Artificial Intelligence within Cybersecurity

The previous section discussed the benefits of AI as well as the various techniques that can address significant technological issues in today's cybersecurity domain. Despite these positive aspects, the concerns and risks from using AI within cybersecurity are as follows:

a. Inability to maintain cybersecurity autonomously: Although there have been huge advances in adapting AI techniques to cybersecurity, security systems are not yet fully autonomous. Since they are not yet able to completely replace human decisions, there are still tasks that require human intervention.[47]
b. Data privacy: AI techniques, like ANNs and DNNs, are becoming more advanced and new techniques emerge regularly—thanks to advances in hardware. The growing need, however, for big data can have a negative side when it comes to data privacy. The analysis of huge amounts of data may cause private as well as public organizations to be concerned about the privacy of their personal data, and some are even unwilling to share this data at all.[48] What personal data is used, why it is used, and how conclusions are reached within AI-based solutions may remain unanswered and may not be transparent for affected organizations.
c. Lack of regulation: Although there are various legal concerns about AI, the one concern that is most prevalent is the loss of human control over the consequences of AI's autonomy. Due to the unique and unforeseeable nature of AI, existing legal frameworks do not necessarily apply to this discipline.[49]

d. Ethical concerns: AI-based security systems increasingly make decisions for human individuals or assist them to do so (e.g., as discussed above in the case of Expert Systems). Considering this development, it is particularly worrisome that these systems do not currently have a moral code. Consequently, the decisions that are made for us are not necessarily the ones that a person would take.[50]

Conclusions

AI is considered as one of the most promising developments in the information age, and cybersecurity arguably is the discipline that could benefit most from it. New algorithms, techniques, tools, and enterprises offering AI-based services are constantly emerging on the global security market. Compared to conventional cybersecurity solutions, these systems are more flexible, adaptable, and robust, thus helping to improve security performance and better protect systems from an increasing number of sophisticated cyberthreats. Currently, deep learning techniques are possibly the most promising and powerful tools in the realm of AI. DNNs can predict cyberattacks in advance, instead of solely preventing them, and might lead to a new phase of cybersecurity.

Despite the promising nature of AI, it has emerged as a global risk for human civilization, while the risks and concerns for its use in cyberspace are justified. Here, four major issues can be identified: the lack of AI's full autonomy, concerns about data privacy, the absence of sufficient legal frameworks, in addition to ethical concerns originating from a missing moral code of autonomous decision-making systems. Due to the fast-growing nature of AI, it is necessary to resolve these related risks and concerns as early as possible. But, given these concerns and that sustainable solutions are not in sight, a socially responsible use of AI within cybersecurity is highly recommended. This could help to mitigate at least some related risks and concerns.

Until now, neither people nor AI alone have proven overall success in cyber protection. Despite the great improvements that AI has brought to the realm of cybersecurity, related systems are not yet able to adjust fully and automatically to changes in their environment; learn all the threats and attack types; and choose and autonomously apply dedicated countermeasures to protect against these attacks. Therefore, at this technological stage, a

strong interdependence between AI systems and human factors is necessary for augmenting cybersecurity's maturity. Moreover, a holistic view on the cyber environment of organizations is required. Cybersecurity is not only a technological issue; it is also about regulation and the way that security risks are dealt with. It is necessary to integrate any technical solutions, relevant processes, and people into an ISA framework to achieve optimal security performance. In the end, it is still the human factor that matters—not (only) the tools.

Notes

1 In 1988, Robert Tappen Morris, a graduate student in computer science, wrote the first computer program, which was distributed via the internet: the Morris Worm. The program was not designed to cause damage, but rather to gauge the size of the internet; a critical error, however, transformed the program, causing it to launch the first denial-of-service attack.

2 About the IDPS weaknesses, see Amjad Rehman and Tanzila Saba, "Evaluation of Artificial Intelligent Techniques to Secure Information in Enterprises," *Artificial Intelligence Review* 42, no. 4 (2014): 1029–1044, especially the section "Performance issues: IDS."

3 Selma Dilek, Hüseyin Çakır, and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," *International Journal of Artificial Intelligence & Applications* 6, no. 1 (2015): 21–39.

4 Enn Tyugu, "Artificial Intelligence in Cyber Defense," in *Proceedings of 3rd International Conference on Cyber Conflict [ICCC], 7–10 June, 2011 Tallinn Estonia*, eds. C. Czosseck, E. Tyugu, and T. Wingfield (Tallinn, Estonia: CCD COE, 2011), pp. 95–105; Xiao-bin Wang, Guang-yuan Yang, Yi-chao Li, and Dan Liu, "Review on the Application of Artificial Intelligence in Antivirus Detection System," *Cybernetics and Intelligent Systems* (2008): 506–509.

5 The Global Challenges Foundation states AI as one of two emerging risks that might threaten mankind in the future. For more, see Dennis Pamlin and Stuart Armstrong, "Global Challenges—Twelve risks that threaten human civilisation," (Global Challenges Foundation: 2015), http://globalchallenges.org/wp-content/uploads/12-Risks-with-infinite-impact.pdf.

6 Stuart Russell, Tom Dietterich, Eric Horvitz, Bart Selman, Francesca Rossi, Demis Hassabis, Shane Legg, Mustafa Suleyman, Dileep George, and Scott Phoenix, "Research Priorities for Robust and Beneficial Artificial Intelligence: An Open Letter," *AI Magazine* 36, no. 4 (2015): 105–114.

7 My Digital Shield, "A History of Cybersecurity: How Cybersecurity Has Changed in the Last 5 Years," October 5, 2015, http://www.mydigitalshield.com/history-cyber-security-cyber-security-changed-last-5-years/.

8 Rehman and Saba, "Evaluation of Artificial Intelligent Techniques."

9 There are various approaches to describe the different stages of a cyberattack. This article refers to the *Cyber Kill Chain*® by Lockheed Martin, which has been widely used by the security community. For more, see www.lockheedmartin.com.
10 Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affairs*, May 7, 2015, http://journal.georgetown.edu/an-integrated-security-approach-the-key-to-cyber-defense/.
11 Tony Sager, "Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention," A SANS Analyst Whitepaper (2014), https://www.sans.org/reading-room/whitepapers/analyst/killing-advanced-threats-tracks-intelligent-approach-attack-prevention-35302.
12 Cyber intelligence is more than the availability of raw data; rather, it provides actionable information of pre-sorted, processed, and evaluated data. For more about cyber threat intelligence and the conceptual delimitation of cyber intelligence and cyber information, see "What Is Cyber Threat Intelligence and Why Do I Need It?" iSIGHT Partners Inc. (2014), http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief1.pdf.
13 Siboni, "An Integrated Security Approach."
14 Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino Júnior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review," *Journal of Network and Computer Applications* 36, no. 1 (January 2013): 25–41.
15 Susan M. Bridges and Rayford B. Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection," *12th Annual Canadian Information Technology Security Symposium* (2000): 109–122.
16 Patel, Taghavi, Bakhtiyari, and Celestino Júnior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review."
17 Rehman and Saba, "Evaluation of Artificial Intelligent Techniques."
18 Sager, "Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention."
19 The Federal Financial Institutions Examination Council developed the Cybersecurity Assessment Tool to help organizations identify their risks and determine their cybersecurity preparedness. The maturity level helps organizations to determine whether their behaviors, practices, and processes can support their cybersecurity preparedness. It also identifies potential actions that would increase this preparedness. For more, see https://www.ffiec.gov/cyberassessmenttool.htm.
20 Amirudin Abdul Wahab, "Facing Cyberattacks in 2016 and Beyond," *The Star*, January 28, 2016, http://www.thestar.com.my/tech/tech-opinion/2016/01/28/facing-cyber-attacks-in-2016-and-beyond/.
21 Rehman and Saba, "Evaluation of Artificial Intelligent Techniques."
22 Linda Ondrej, Todd Vollmer, and Milos Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures," *2009 International Joint Conference on Neural Networks* (Atlanta, GA, 2009): 1827–1834.

23 Yoshua Bengio, "Learning Deep Architectures for AI," *Foundations and Trends® in Machine Learning* 2, no. 1 (2009): 1–127.
24 Tyugu, "Artificial Intelligence in Cyber Defense."
25 "Fixed" algorithms use hard wired logic, on decision level, for reasoning about data. See Ibid.
26 Olin Hyde, "Machine Learning for Cybersecurity at Network Speed & Scale," an Invitation to Collaborate on the Use of Artificial Intelligence against Adaptive Adversaries, ai-one (2011), www.ai-one.com/.
27 "Noise" refers to inaccurate or irrelevant information in the collected data.
28 INFOSEC Institute, "Cybersecurity and Artificial Intelligence: A Dangerous Mix," February 24, 2015, http://resources.infosecinstitute.com/cybersecurity-artificial-intelligence-dangerous-mix.
29 A cognitive cyber entity can be understood as a single program, either software or hardware, that has human-like cognitive capabilities. In the realm of AI, the cognitive abilities of an intelligent agent would include perception of the cyber environment, acquisition, analysis of data gathered across cyberspace, and reasoning about that data.
30 Stan Franklin and Art Graesser, "Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents," *Third International Workshop on Agent Theories, Architectures, and Languages* (London: Springer-Verlag, 1997): 21–35.
31 Alessandro Guarino, "Autonomous Intelligent Agents in Cyber Offence," in *5th International Conference on Cyber Conflict*, eds. K. Podins, J. Stinissen, and M. Maybaum (Tallinn, Estonia: NATO CCD COE, 2013): 377–388.
32 Tyugu, "Artificial Intelligence in Cyber Defense."
33 Xia Ye and Junshan Li, "A Security Architecture Based on Immune Agents for MANET," *International Conference on Wireless Communication and Sensor Computing* (2010): 1–5.
34 Christian Bitter, David A. Elizondo, and Tim Watson, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection," *World Congress on Computational Intelligence* (2010): 949–954.
35 Ibid.
36 Tyugu, "Artificial Intelligence in Cyber Defense."
37 Packet headers contain attributes like the length of the transferred data, the network protocol type, or the source and destination addresses of a data packet. Therefore, the packet header carries information that can be sufficiently used to differentiate normal network behavior from intrusion attempts.
38 Ondrej, Vollmer, and Manic, "Neural Network Based Intrusion Detection System."
39 Bitter and others, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection."
40 The experimental simulations of malware detection emphasized worm and spam detection. For more, see Dima Stopel, Robert Moskovitch, Zvi Boger, Yuval Shahar, and Yuval Elovici, "Using Artificial Neural Networks to Detect Unknown

Computer Worms," *Neural Computing and Applications* 18, no. 7 (2009): 663–674.

41 Geoffrey E. Hinton, Simon Osindero, and Yee-Whye Teh, "A Fast Learning Algorithm for Deep Belief Nets," *Neural Computation* 18, no. 7 (2006): 1527–1554.

42 Victor Thomson, "Cyber Attacks Could Be Predicted With Artificial Intelligence," *iTechPost*, April 21, 2016. www.itechpost.com/articles/17347/20160421/cyber-attacks-predicted-artificial-intelligence-help.htm.

43 Tyugu, "Artificial Intelligence in Cyber Defense."

44 Serena H. Chen, Anthony J. Jakeman, and John P. Norton, "Artificial Intelligence Techniques: An Introduction to Their Use for Modelling Environmental Systems," *Mathematics and Computers in Simulation* 78, no. 2–3 (2008): 379–400.

45 Ibid.

46 Debra Anderson, Thane Frivold, and Alfonso Valdes, "Next-Generation Intrusion Detection Expert System (NIDES): A Summary," SRI International, Computer Science Laboratory: May 1995.

47 Katherine Noyes, "A.I. + Humans = Serious Cybersecurity," *Computerworld*, April 18, 2016, www.computerworld.com/article/3057590/security/ai-humans-serious-cybersecurity.html.

48 Tom Simonit, "Microsoft and Google Want to Let Artificial Intelligence Loose on Our Most Private Data," *MIT Technology Review*, April 19, 2016, https://www.technologyreview.com/s/601294/microsoft-and-google-want-to-let-artificial-intelligence-loose-on-our-most-private-data/.

49 Bernd Stahl, David Elizondo, Moira Carroll-Mayer, Yingqin Zheng, and Kutoma Wakunuma, "Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics," *The 2010 International Joint Conference on Neural Networks (IJCNN)*: 1–8.

50 Nick Bostrom, "Ethical Issues in Advanced Artificial Intelligence," in *Cognitive, Emotive and Ethical Aspects of Decision Making in Humans and in Artificial Intelligence*, eds. Iva Smit and George E. Lasker (Windsor, ON: International Institute for Advanced Studies in Systems Research / Cybernetics, 2003) 2: 12–17.

Pedal to the Metal? The Race to Develop Secure Autonomous Cars

Andrew Tabas

The advent of Autonomous Vehicles (AVs) will have profound effects on car ownership, transportation, and security. It is already possible to hack into individual cars through their entertainment and navigation systems. The connecting of AVs to networks will make it possible to hack them on a large scale. Policymakers should act now to implement both technical and legal security mechanisms. Potential solutions include the establishment of a system of certificates, an effort to establish an air gap between different computer networks in the vehicles, and the creation of laws that penalize hackers. Still, manufacturers should not be deterred by the risks of AVs. Instead, they should race ahead in the development of this potentially lifesaving technology.

Keywords: autonomous vehicles, self-driving cars, V2V, V2I, intelligent transportation systems, Internet of Things, public key encryption, cybersecurity, hacking, air gap

Introduction

"Get them!" In his 1953 short story "Sally," Isaac Asimov tells the story of "positronic" cars that drive themselves. The cars also communicate (in an autonomous vehicle network), defend themselves (a response to security concerns), and kill (demonstrating the ethical problems at play with autonomous

Andrew Tabas (Bachelor of Science in Foreign Service, Georgetown University, 2016) is a research analyst at the Cadmus Group.

vehicles).[1] "Sally" is a good starting point for a discussion of autonomous vehicles (AVs) because the story highlights issues that technology companies and car manufacturers face today.

What vulnerabilities could threaten AVs and their drivers? How can manufacturers and policymakers respond to these vulnerabilities? AVs have unique vulnerabilities that necessitate innovative security solutions. First, AVs depend on sensors for input. These sensors can be tricked, risking the security of the vehicle and its passengers. Second, AVs gain information for life-and-death situations in a system that relies on cloud infrastructure. GPS systems, critical software updates, and communication with other vehicles all rely on the cloud and could be vulnerable to hacks. Third, a future network of AVs could be vulnerable to large-scale exploits and attacks. Manufacturers should embrace these challenges, as the winner of the race to develop safe and secure AVs will save lives and change the world.

The Technology

It is useful to distinguish between "autonomous cars" and "self-driving cars." Autonomous cars will be able to drive themselves in certain conditions, but will maintain the capability to be driven by people. The development of autonomous cars benefits automakers because they can advertise that their vehicles have sophisticated technology. Autonomous cars must be capable of "graceful degradation," or a smooth transition back to a human driver.[2] Humans, on the other hand, will not be able to drive self-driving cars. These vehicles will look markedly different from today's cars, as they will lack steering wheels, pedals, and mirrors. They could form "a fleet of shared vehicles" that will end traditional car ownership.[3] In that case, they would threaten traditional car manufacturers as family cars become a luxury item. Indeed, Tesla has proposed that owners of AVs could make money by contributing their cars to the fleet when they are not using them, an action that would help to make AVs more affordable.[4]

The National Highway Traffic Safety Administration (NHTSA) has specified five "levels" of automation: "No-Automation" (0); "Function-Specific Automation" (1); "Combined Function Automation" (2); "Limited Self-Driving Automation" (3); and "Full Self-Driving Automation" (4). An increased level represents more features working together without the driver's input. Level Zero represents traditional cars. At Level One, the car

can perform specific tasks by itself. At Level Two, the car's autonomous capabilities can interact, but the driver still needs to be active. For example, a Level Two car could combine "adaptive cruise control" and "lane centering." Level Three vehicles can drive themselves in certain environments, but the driver must stay attentive.[5] It may be difficult, however, for drivers to focus when the AV is doing most of the work. At Level Four, the driver does not need to remain attentive or even stay in the vehicle.[6] Level Four cars, which represent the "self-driving cars" described above, will not need steering wheels, brake pedals, or other expected components of cars.

In traditional cars, human drivers are the link between vehicles and their environment. Drivers watch traffic signs and signals, monitor road conditions, avoid other vehicles, communicate with other drivers, and navigate. To fulfill these functions, AVs employ sensors, vehicle-to-vehicle (V2V) communications, and vehicle-to-infrastructure (V2I) communications. AVs, like other objects in the Internet of Things (IoT), rely on cloud infrastructure.

Anderson and others describe the "sensor suites" that provide information to AVs. First, cameras gather data about the outside world.[7] Cameras are limited by weather conditions and by the capability of software that converts images to data.[8] Second, AVs rely on sensors. Radar and lidar both emit a signal and track the time that it takes for the signal to bounce off of an object and return to the sensor to determine distance.[9] Both technologies have limitations because some surfaces do not adequately reflect radio waves and light.[10] Ultrasonic sensors detect nearby objects while infrared sensors detect objects at night.[11] Third, AVs can use GPS and internal navigation systems (INS) for location information.[12] INS relies on gyroscopes, altimeters, and accelerometers.[13] Finally, AVs can have access to maps that include information on traffic signals.[14] For example, Google has designed vehicles that collect information and build virtual maps of road features as they drive.[15]

AVs communicate with vehicular ad-hoc networks (VANETs).[16] VANETs "are the basis for intelligent transportation systems (ITSs)."[17] V2I technologies share information on traffic signals and other external factors with cars. These systems help AVs to understand the world around them. Bluetooth could be used to improve V2I communications.[18] In addition, V2V technologies enable cars to share information with each other about their own location and speed to reduce the likelihood of a crash. AVs communicate with each other using dedicated short-range communications (DSRC).[19] The US Government

Accountability Office recently released a study on the potential application of technology to cars with human drivers.[20]

AVs use a "sense-plan-act design."[21] Cars detect information, run algorithms to determine the best response, and execute the necessary action. AVs are an example of "Massively Integrated Systems of Smart Transducers" (MIST), which "use cloud concepts to acquire information, sense their surroundings, and actively intervene in situations to effect desirable outcomes."[22]

AVs present a unique challenge because they must, at all costs, ensure the safety of their passengers. Engineers must ensure that sensors are effective in all types of weather and traffic conditions. They must protect these sensors from outside interference, which could threaten the safety of the passengers in the AV and in neighboring vehicles; cybersecurity therefore becomes a key concern in the production of AVs.

Towards a Collective Vehicular Network

V2V and V2I communications enable the creation of a "collective vehicular network." Humans, cars, and infrastructure communicate in this network to create efficient vehicles. Cars learn of weather conditions and other information through cloud infrastructure. Cars will need to deal with human drivers at first, but eventually will communicate solely with each other. In a network without human drivers, programmers will need to determine methods to increase the flow of traffic. Riener predicts that the future of autonomous cars is a shared fleet in which a passenger can order a car for a trip and then allow the car to return to a central location.[23]

Like sensors, V2V and V2I communication present cybersecurity challenges. Malicious communication could conceal or invent road hazards. These imagined hazards would cause the car to behave erratically. More advanced hackers could use the AV's communications system to access the car's central computer and gain control of the AV's steering and braking. It will be necessary, therefore, to secure the external communications of the AVs.

Current Industry Trends

In the race to develop secure AVs are both traditional automakers and technology companies. Companies include Volkswagen, Mercedes-Benz, Tesla, Bosch, Uber, Lockheed Martin, Google, Apple, and others. Development has extended to trucks and military vehicles.[24] Elon Musk, the founder of Tesla,

recently predicted that most cars will be autonomous by 2030 or 2035.[25] Uber recently established a lab in Pittsburgh in which a large contingent of Carnegie Mellon University graduates is researching self-driving cars. Meanwhile, Google has sent cars cruising through 300,000 miles without any accidents caused by its cars.[26]

Traditional auto manufacturers or technology companies have different strengths, leading to debates about which type of developer will be more successful. Traditional automotive companies are better equipped to handle challenges that are unique to auto manufacturers and can gradually phase in new features. Meanwhile, technology companies may face a user acceptance problem if they jump into the automotive market. At the same time, one Google executive argued that its plan to move into selling fully autonomous cars could prove to be a more effective business strategy.[27]

Manufacturers must develop "user acceptance" of AVs through innovative design, advanced security, and well-publicized statistics. First, self-driving cars (at Level 4 on the NHTSA scale) could replace the steering wheel with a display that inspires confidence in the car.[28] Second, security experts must consider the risks of data exploitation and direct attack. A congressional hearing on the subject acknowledged that "hacking could threaten widespread acceptance" of AVs as concerns grow over data security and personal safety.[29] Users could be concerned that their cars' V2V communications are not protected.[30] They could also have concerns about attacks on the safe operation of the car itself. Third, manufacturers could stress the fact that AVs are safer than human-driven vehicles.[31] Car crashes, 93 percent of which are caused by "human error," took 34,080 lives in 2012.[32] These violent events cost approximately $230 billion per year.[33] AVs could help to move toward the "ultimate goal" of being "the safest and most efficient transportation system imaginable."[34] However, if an AV does crash, the media will discuss the event more than it would discuss an ordinary car accident. For example, the first-ever death in an AV crash occurred in June 2016, when a Tesla crashed into a turning tractor trailer.[35] Although the crash received significant media coverage, Tesla was quick to reassure the public that, even after the crash, the autopilot feature has a lower death rate than human drivers.[36]

It is also possible to promote user acceptance by stressing the other benefits of AVs. These include greater mobility for people who are unable to drive, a smaller dependence on parking, and potential environmental

benefits.[37] Manufacturers should emphasize that these benefits outweigh the potential increase in total miles traveled and the likely decrease in the number of professional driving jobs.[38]

Vulnerabilities

Today, large-scale hacks are both inefficient and expensive because cars use different computer systems. As cars become integrated through advanced communications systems and vehicular networks, however, large-scale hacks may become possible. Moreover, hacks of individual cars are already possible; two hackers, for example, were able to control the steering, braking, and acceleration of a jeep through the car's Uconnect system. The jeep's entertainment system was connected to its steering and breaking controls through its computer network, known as the "CAN bus."[39] AVs have even more connections with the outside world and greater computerized control of the car's systems than the hacked jeep, increasing the vulnerability of these types of cars. Uber recently hired the two hackers to improve its own vehicles' security.[40]

Car manufacturers must proactively protect AVs from hacks directed at software updates, sensors, and communications networks. First, although software updates are necessary for AVs to function effectively, they are also a major vulnerability.[41] If the updates are installed online, the system becomes even more at risk.[42] Second, AVs' sensors can be fooled. If an AV mistakenly detects a pedestrian on the road, the car could suddenly stop.[43] Indeed, lidar sensors can be fooled with a sixty-dollar laser.[44] There is also a risk that drivers could "jailbreak" their cars, or hack their own vehicles to change the way that they behave.[45] Owners who "jailbreak" their cars would increase control, but risk security.[46] That risk increases when a jailbroken car drives near an ordinary car that expects it to act in a certain way. Finally, the fact that AVs will be connected to each other by communications networks will cause additional vulnerabilities. Attacks on V2V, V2I, and GPS can target safety, user acceptance, and privacy.[47] V2V communication is therefore vulnerable to both computer network exploit (CNE) and computer network attack (CNA). CNE against an AV's communications could target the victim's privacy.[48] Data about where a certain driver traveled could then be used against him or her. CNA against an AV could generate and report fictional illegal activity, causing unfortunate repercussions for the driver.[49] Hackers

of V2V communications can target keys, software, sensors, and outgoing communications.[50] DoS attacks could overload the car with information or prevent the car from sending signals.[51]

Lacey identifies three types of attack against V2V and V2I communications. A hacker can use "message linking" and track the V2V "Basic Safety Message" to discover the location of a car. In a "framing attack," the hacker first steals the car's online certificate, then sends incorrect messages to show fictional illegal driving. A "framing attack" could cause the arrest of an innocent driver. In a "Sybil attack," a hacker steals certificates of many cars, then sends messages from each car that point to a single car's illegal driving.[52] A "Sybil attack" could also frame a law-abiding driver. Each of these vulnerabilities represents an obstacle on the race course to develop secure AVs. As manufacturers and technology companies find new solutions, they will move closer to victory.

Hacking Motivations

Terrorism is a major threat to AVs. For an aspiring international terrorist with technical expertise, hacking one or multiple AVs would be an excellent way to create visible carnage. Even a small-scale hack of a few cars could shut down transportation. An attack would cause fear among commuters in AVs and traditional vehicles alike because, if a hacked AV is on the road, no car is safe. This fear could result in a decline in car usage and a slowdown of the US economy. Indeed, after the attacks of September 11, 2001, airplane travel decreased "dramatically" and did not recover until 2004.[53] AVs could also be a useful way for terrorists to assassinate specific targets. A well-disguised attack on a single car may register as a technical malfunction.

Hackers could also target AVs to try to blackmail consumers or the US government. If a consumer received a notification from their car that the car would deliberately crash unless money was sent to an online account, the consumer may be forced to comply. Similarly, a criminal organization could tell the US government that it had hacked several unidentified cars. It could then force the government to meet its demands or threaten to launch a massive attack. Luckily, an economically motivated hacker would find the process of hacking an AV to be expensive.[54] Hacking AVs will only be attractive if hackers can find a way to make a profit.[55] In addition, as one white hat hacker points out, the people who have the technical knowledge

necessary to hack cars' communications systems generally do not want to kill people.[56] A graver risk is political blackmail. The group Anonymous, for example, could hack AVs to demand that the US government change certain policies. Foreign governments are less of a threat than terrorists and criminals. They could target AVs' communications network, but the resulting disruption of the US economy would likely affect their own economy as well. It is risky, however, to rely on other governments to make this calculation.

Potential Solutions

To reduce the probability of cyberattacks on AVs, it is necessary to secure cloud infrastructure, protect telecommunications, and examine the vulnerabilities specific to AVs. The final category includes a range of technical and legal solutions.

Protecting cloud infrastructure from cyberattacks is essential for the security of AVs. To secure the cloud, technology companies should be required to follow "best practices of application security" to be granted access to the network.[57] Rigorous testing and reporting practices will help to ensure a secure network.[58] Finally, cybersecurity teams must act like "firefighters," ready to respond to cyberattacks quickly.[59]

Protecting telecommunications, including V2V and V2I, is essential for privacy and security. Education, collaboration that respects privacy rights, laws, and leadership can protect telecommunications infrastructure from cyberattacks.[60] For effective V2V and V2I communication, vehicles can send out one-way, unencrypted "Basic Safety Messages" that can be read by nearby vehicles, in addition to two-way, encrypted "trusted and secure communications."[61] One Israeli startup called Argos, for example, is developing a way to determine which messages are legitimate and which are malicious.[62]

There are also potential solutions that are specific to AVs. These solutions, when combined, reduce the likelihood of a successful attack against an AV. First, developers will need to have a clear understanding of traffic patterns and the way that AVs interact with other cars, cyclists, and pedestrians. This understanding will enable them to distinguish normal driving behavior from hacked behavior. Second, they will need to ensure that a given AV or software update source can be positively identified. Public Key Infrastructure (PKI) could manage the identifying certificates of AVs online.[63] A "Certificate

Authority" would be responsible for assigning online certificates to AVs.[64] The system that assigns those certificates could be "centralized, decentralized, or hybrid."[65] The certificates would identify cars that belong in the system.[66] Next, companies will need to ensure that cars can identify legitimate software updates. AVs can distinguish between legitimate and malicious software updates through "handshake" mechanisms.[67] There are also a range of technical solutions that enable cars' computer systems to make sure that they are connected to the correct car and that they are running legitimate software.[68] "Plausibility checks" limit the software that can run on a car's "electronic control unit" (ECU).[69] "Component identification" pairs one ECU with one car.[70] Another piece of software attempts to detect unusual data.[71]

Third, AV developers should separate essential and nonessential computer systems. The Jeep hack demonstrated the vulnerability of cars whose functions are all linked electronically. Camek and others recommend that car manufacturers build cars with "multiple independent layers of security" (MILS) that are "adaptive" and "distributed." "MILS architecture" establishes a barrier between essential and nonessential computers in the car. The separation of computer systems can prevent a virus from reaching a car's essential functions.[72] A "distributed" system would allow MILS architecture to function across multiple computers. An "adaptive" system can be updated with new capabilities.[73] These elements will help to reduce the likelihood of attack on future AVs.

Fourth, manufacturers should explore additional technical solutions. "Black boxes," which were originally used in airplanes, can record data on crashes without necessarily recording private GPS data.[74] This data can be used to understand mistakes that led to a crash and could provide a clue as to whether the vehicle was hacked. AVs should also be equipped with a "safe mode" in which the car's autonomous features can be disabled.[75] In the event of a hack, a driver could then safely gain control of the vehicle. For a "safe mode" to exist, AVs would need to maintain the traditional steering wheel and brake pedal. Manufacturers should also adhere to industry standards and extensively test their vehicles.[76]

Fifth, while many efforts have been taken to protect AVs from technical challenges, it is useful to explore legal solutions. The right laws could both deter hackers and make hacking more difficult. Indeed, various states are already implementing laws about the testing of autonomous vehicles.[77] The

states should aim to implement laws that require AV makers to follow security best practices. State and national legislatures can also make legislation that protects certificates. As it is impossible to design a car whose hardware is tamper-proof, laws will need to deter people from stealing software keys once they have physical access to a vehicle.[78] In addition, they can develop laws that protect existing autonomous systems, such as those used by air control systems. These laws could be extended to cover AVs as they become more common.

Sixth, courts and private companies can also play a role. Courts must determine how to respond to accidents that are caused by hacks. Companies that gather data on AVs should be legally responsible to protect that data.[79] The requirements will encourage the companies to invest in data security.

Ethical Dilemmas

AVs apply cloud infrastructure to life-and-death situations and therefore raise many ethical questions. While a full ethical discussion is beyond the scope of this paper, it is useful to review some of the existing literature and ongoing questions. Ethical systems can focus on utilitarianism, rights, justice, the "common good," or virtues.[80] I begin with a utilitarian approach because AVs seek to save as many lives as possible. According to Alexander Kott, "self-driving cars will kill people, but fewer people."[81] From a utilitarian point of view, the obvious choice is to implement autonomy. Turck goes a step further and argues that an AV should be programmed not only to save lives, but also to keep traffic flowing smoothly for millions of other drivers.[82]

Since AVs' algorithms are written in advance, every tradeoff in terms of lives and convenience is made ahead of time. When coders program AVs' algorithms, they will need to make the algorithms "consistent," avoid "public outrage," and "not [discourage] buyers."[83] AV makers will need to choose between killing pedestrians and drivers. Frowe argues that by choosing to get into a car, a driver assumes responsibility and therefore should risk being killed before a pedestrian.[84] Psychologists and polling data will be required to construct acceptable algorithms, as individuals could be reluctant to get in a utilitarian vehicle that may kill them but may save a pedestrian.[85] Consistency in algorithms is also essential; otherwise, there could be economic discrimination as those capable of purchasing cars that protect the driver will do so.

It is also challenging to examine who is responsible for a crash. As AVs become more common, it will be necessary to determine whether manufacturers or the person in the front seat of the AV is responsible.[86] The answer could depend on whether the car is autonomous (Level 3) or self-driving (Level 4). Finally, there is the issue of an autonomous vehicle network that takes away individual freedoms. If the government controls the network, it could determine not only drivers' speed, but also their destination. A collective vehicular network could therefore give rise to a government that controls individuals' transportation.[87]

Implications and Areas of Further Research

So, should automakers throw in the towel? Are the unique security and technical challenges so great that technology companies and car manufacturers should put AVs on hold until they are more secure? Absolutely not. AV developers should continue to race ahead because AVs, even with their imperfections, can prevent crashes and save lives. Elon Musk, the founder of Tesla, recently made this point. He wrote that the company is not waiting to release AVs because "when used correctly, [autonomy] is already significantly safer than a person driving by themselves and it would therefore be morally reprehensible to delay release simply for fear of bad press or some mercantile calculation of legal liability."[88] Meanwhile, as AVs develop, their designers must continue to develop more effective security measures.

AVs have many other implications that could lead to future research. These include the controversy over the right to use DSRC wireless communications;[89] the cybersecurity of drones;[90] AV conformance to imperfect human driving behavior;[91] and the growth of a new in-car entertainment industry. Legal concerns include responsibility for accidents;[92] the legality of police-tracking services such as those offered by Waze; the effect of AVs on car insurance companies; and the risk of someone manipulating AV data to create false evidence.

As we speed toward a world of the Internet of Things, we might want to fasten our seatbelts.

Notes

1 Isaac Asimov, "Sally," in *Nightfall Two* (Frogmore: Granada, 1976).
2 James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A. Oluwatola, *Autonomous Vehicle Technology: A Guide for Policymakers* (Santa Monica: RAND, 2014), p. 66.
3 "Why Autonomous and Self-Driving Cars Are Not the Same," *Economist*, July 1, 2015, http://www.economist.com/blogs/economist-explains/2015/07/economist-explains.
4 Elon Musk, "Master Plan Part Deux," *Tesla* (blog), July 20, 2016, https://www.tesla.com/blog/master-plan-part-deux.
5 "US Department of Transportation Releases Policy on Automated Vehicle Development," *NHTSA*, May 30, 2013, http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development.
6 Ibid.
7 Anderson and others, *Autonomous Vehicle Technology*, p. 60.
8 Ibid., p. 61.
9 Ibid., pp. 61–62.
10 Ibid.
11 Ibid., p. 62.
12 Ibid., p. 64.
13 "How Does a Self-Driving Car Work?" *Economist*, April 29, 2013, http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-self-driving-car-works-driverless?fsrc=scn/fb/wl/bl/tr/st/howdoesaself-drivingcarwork.
14 Anderson and others, *Autonomous Vehicle Technology,* p. 64.
15 Ibid.
16 Christoph Ponikvar and Hans-Joachim Hof, "Overview on Security Approaches in Intelligent Transportation Systems: Searching for Hybrid Trust Establishment Solutions for VANETs," *Secureware (2015): The Ninth International Conference on Emerging Security Information, Systems and Technologies*, eds. Rainer Falk, Carla Merkle Westphall, and Hans-Joachim Hof (Wilmington, DE: IARIA, 2015), http://toc.proceedings.com/27725webtoc.pdf.
17 Ibid., p. 1.
18 Anderson and others, *Autonomous Vehicle Technology,* p. 80.
19 Douglas Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems: Development, Challenges and Security Proposals* (New York: Nova Science, 2014), p. 10.
20 United States Government Accountability Office, "Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist," (2013).
21 Anderson and others, *Autonomous Vehicle Technology*, p. 58.
22 Jerry L. Archer, "International Engagement on Cyber V: Securing Critical Infrastructure," *Georgetown Journal of International Affairs* (2015), p. 168.

23 Andreas Riener, "Who Cares about Trust, Grade of Traveling and Quality of User Experience in a World of Autonomous Cars?" *AutomotiveUI '14*, Adjunct Proceedings of the Sixth International Conference on Automotive User Interfaces and Interactive Vehicular Applications (2014), pp. 1–3.
24 Nick Lavars, "Self-driving Truck Hits the Highway in World First," *New Atlas,* October 4, 2015, http://newatlas.com/daimlers-production-autonomous-truck-debuts-public-roads/39701/; David Sedgwick, "Army Eyes Self-Driving Convoys," *Automotive News*, August 4, 2015, https://www.autonews.com/article/20150804/OEM06/308059984/army-eyes-self-driving-convoys.
25 Benjamin Snyder, "Tesla CEO Elon Musk Just Told Us When All Cars Will Be Self-Driving," *Fortune,* November 4, 2015, http://fortune.com/2015/11/04/tesla-elon-musk-self-driving-cars/.
26 United States Government Accountability Office, "Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist," (2013), p. 7.
27 "Upsetting the Apple Car," *Economist*, February 21, 2015, http://www.economist.com/news/business/21644149-established-carmakers-not-tech-firms-will-win-race-build-vehicles.
28 Nikhil Gowda, Wendy Ju, and Kirsten Kohler, "Dashboard Design for an Autonomous Car," *AutomotiveUI '14*, Adjunct Proceedings of the Sixth International Conference on Automotive User Interfaces and Interactive Vehicular Applications (2014), pp. 1–4.
29 United States Government Accountability Office, "Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist," (2013), p. 8.
30 Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems*, p. 25.
31 Anderson and others, *Autonomous Vehicle Technology,* pp. 15–16.
32 United States Subcommittee on Highways and Transit, "How Autonomous Vehicles Will Shape the Future of Surface Transportation," (2013), p. vii.
33 Ibid.
34 Ibid., p. 7.
35 The Tesla Team, "A Tragic Loss," *Tesla* (blog), June 30, 2016, https://www.tesla.com/blog/tragic-loss.
36 Ibid.
37 Anderson and others, *Autonomous Vehicle Technology,* p. 9.
38 Ibid., p. xvii.
39 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired,* July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
40 Roberto Baldwin, "Jeep Hackers Get New Jobs at Uber's Autonomous-car Lab," *Egadget*, August 28, 2015, https://www.engadget.com/2015/08/28/uber-jeep-hackers/.
41 Anderson and others, *Autonomous Vehicle Technology,* p. 70.

42 Ibid.
43 Ibid., p. 71.
44 Anna Peel, "Self-Driving Cars Can Be Disabled with Lasers," *ValueWalk*, September 8, 2015, http://www.valuewalk.com/2015/09/self-driving-cars-can-be-disabled-with-lasers/.
45 Anderson and others, *Autonomous Vehicle Technology,* p. 71.
46 Ibid., p. 71.
47 Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems*, p. 54.
48 Ibid., p. 72.
49 Ibid.
50 Ibid., pp. 68–69.
51 Ibid., p. 69.
52 Ibid., pp. 72–73.
53 United States Department of Transportation, Research and Innovative Technology Administration, "Air Travel Since 9/11," *Bureau of Transportation Statistics Issue Brief,* no. 13 (December 2005), http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/special_reports_and_issue_briefs/issue_briefs/number_13/html/entire.html.
54 James Guy and Mat Greenfield, "Can Driverless Cars Ever Be Made Hack-Proof?" *Guardian,* March 9, 2015, https://www.theguardian.com/technology/2015/mar/09/driverless-cars-safe-hackers-google.
55 Ibid.
56 Ibid.
57 Jerry L. Archer, "Dynamic and Effective Security in the Rapidly Evolving Global Cloud Computing Cyberspace," *Georgetown Journal of International Affairs* (2015), p. 173.
58 Ibid., 174.
59 Ibid., 175.
60 Tarek Saadawi and Haidar Chamas, "Securing Telecommunications Infrastructure against Cyber Attacks," *Georgetown Journal of International Affairs* (2015): 58–69.
61 Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems,* p. 64.
62 Kobe Liani, "Israeli Start-Up Will Protect Your Car [from] Cyber Terrorism," *Walla*, March 23, 2015, http://cars.walla.co.il/item/2839940.
63 Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems,* p. 63.
64 Ibid., p. 81.
65 Christoph Ponikwar and Hans-Joachim Hof, "Overview on Security Approaches in Intelligent Transportation Systems: Searching for Hybrid Trust Establishment Solutions for VANETs," *SECUREWARE* (2015): 160–165, https://www.thinkmind.org/download.php?articleid=securware_2015_8_10_30019.
66 Ibid.

67 Anderson and others, *Autonomous Vehicle Technology*, p. 70.
68 Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems,* p. 79.
69 Ibid., p. 78.
70 Ibid., p. 79.
71 Ibid.
72 "Five Star Automotive Cyber Safety Program," I Am the Cavalry, February 2015, https://www.iamthecavalry.org/domains/automotive/5star/.
73 Alexander Georg Camek, Christian Buckl, and Alois Knoll, "Future Cars: Necessity for an Adaptive and Distributed Multiple Independent Levels of Security Architecture," *HiCoNS* '13, Proceedings of the Second ACM International Conference on High Confidence Networked Systems (2013), pp. 17–24.
74 "Five Star Automotive Cyber Safety Program."
75 Ibid.
76 Ibid.
77 Anderson and others, *Autonomous Vehicle Technology,* pp. 41–52.
78 Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems*, p. 77.
79 Jerry L. Archer, "International Engagement on Cyber V: Securing Critical Infrastructure," *Georgetown Journal of International Affairs* (2015), p. 174.
80 Manuel Velasquez, Dennis Moberg, Michael J. Meyer, Thomas Shanks, Margaret R. McLean, David DeCosse, Claire André, and Kirk O. Hanson, "A Framework for Thinking Ethically," *Markkula Center for Applied Ethics,* August 1, 2015, https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-framework-for-ethical-decision-making.
81 Alexander Kott, Lecture at Georgetown University, Washington, DC, 2015.
82 Mitch Turck, "An Autonomous Car Might Decide You Should Die," *Backchannel*, March 10, 2015, https://backchannel.com/reinventing-the-trolley-problem-85f3d1730756#.lnpj44f1l.
83 Jean-François Bonnefon, Azim Shariff, and Iyad Rahwan, "Autonomous Vehicles Need Experimental Ethics: Are We Ready for Utilitarian Cars?" October 12, 2015, ArXiv.org, Cornell University, arXiv:1510.03346v.1 [cs.CY], http://arxiv.org/pdf/1510.03346v1.pdf.
84 Olivia Goldhill, "Should Driverless Cars Kill Their Own Passengers to Save a Pedestrian?" *Quartz*, November 1, 2015, http://qz.com/536738/should-driverless-cars-kill-their-own-passengers-to-save-a-pedestrian/.
85 Bonnefon and others, "Autonomous Vehicles Need Experimental Ethics."
86 Alexander Hevelke and Julian Nida-Rümelin, "Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis," *Science and Engineering Ethics* 21, no. 3 (2015): 619–630.
87 Interview by the author with Fr. Dennis McManus, December 8, 2015.
88 Elon Musk, "Master Plan Part Deux," *Tesla* (blog)*,* July 20, 2016, https://www.tesla.com/blog/master-plan-part-deux.

89 Anderson and others, *Autonomous Vehicle Technology,* p. 80.

90 Jon Fingas, "The US Navy Wants to Protect Its Drones against Hacks," *Egadget*, May 20, 2015, https://www.engadget.com/2015/05/20/us-navy-wants-hack-resistant-drones/.

91 Matt Richtel and Conor Dougherty, "Google's Driverless Cars Run into Problem: Cars with Drivers," *New York Times*, September 1, 2015, http://www.nytimes.com/2015/09/02/technology/personaltech/google-says-its-not-the-driverless-cars-fault-its-other-drivers.html?_r=0.

92 "Safer at Any Speed?" *Economist*, March 3, 2012, http://www.economist.com/node/21548992.

Cyber, Intelligence, and Security

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for ***Cyber, Intelligence, and Security***, a new peer-reviewed journal, published three times a year in English and Hebrew. The journal is edited by Gabi Siboni, Head of the Cyber Security Program and the Military and Strategic Affairs Program at INSS.

Articles may relate to the following issues:

- Global policy and strategy on cyber issues
- Cyberspace regulation
- National cybersecurity resilience
- Critical infrastructure cyber defense
- Cyberspace force buildup
- Ethical and legal aspects of cyberspace
- Cyberspace technologies
- Military cyber operations and warfare
- Military and cyber strategic thinking
- Intelligence, information sharing, and public-private partnership (PPP)
- Cyberspace deterrence
- Cybersecurity threats and risk-analysis methodologies
- Cyber incident analysis and lessons learned
- Techniques, tactics, and procedures (TTPs)

Articles submitted for consideration should not exceed 6,000 words (including citations and footnotes), and should include an abstract of up to120 words and up to ten keywords. Articles should be sent to:

Hadas Klein
Coordinator, ***Cyber, Intelligence, and Security***
Tel: +972-3-6400400 / ext. 488
Cell: +972-54-4510411
hadask@inss.org.il