Information-Sharing Challenges in an Intra-Sectorial Environment

Gabi Siboni and Hadas Klein

Information sharing in cyberspace includes the sharing of attack methods, tools and means of attack, targets of an attack, weaknesses discovered, and ways of dealing with threats. Information sharing constitutes a strategic defensive principle. It is aimed at enhancing general strength in cyberspace. Various and diverse information-sharing initiatives are currently operating in Israel and throughout the world, but they are not as effective as they could be.

This article addresses a number of economic and political challenges facing intra-sectorial information-sharing initiative, and examines the extent of their influence, and gives examples of similar challenges in other fields. Finally, we make recommendations in order to minimize the effects of the challenges imposed upon the design and implementation of information-sharing plans in an intra-sectorial environment.

Keywords: cyber security, cooperation, information sharing, privacy, regulation, information security, trust, competition, "free-rider problem"

Introduction

One of the developing principles for strengthening cyber defense is the sharing of concrete and reliable information about existing weaknesses,[1] methods of attack, identification of attackers and motives, and so forth. This sharing is designed to enable the party receiving the information to quickly put defenses in place, thereby preventing the threat of attack from spreading. There should be a model for information sharing among organizations operating in the same market sector and exposed to similar

Dr. Gabi Siboni is the head of Cyber Security Program at the Institute for National Security Studies. Ms. Hadas Klein is the Cyber Security Program Manager at the Institute for National Security Studies.

threats from within their own sector due to having a common denominator, such as political affiliation, common enemies, and so forth or threats from other sectors. This is in addition to information sharing between the private and government sectors as well as state authorities from various countries. More comprehensive information sharing will create better defenses and enable more effective handling of cyberattacks.[2]

Information sharing contributes to the strengthening of general cybernetic resilience[3] at all stages of a cyberattack – from the early states in which the attacker gathers intelligence in order to locate his target to the advanced stages in which the attack actually takes place. Effective and extensive information sharing can contribute to better defense against a cyberattack,[4] among other things, by keeping early-warning mechanisms up-to-date, precise, and relevant; supporting actions to prevent cyber threats from being implemented; improving detection efforts in order to identify an attack at an early stage; facilitating precise analysis of the extent of the damage; and improving reaction and recovery processes when an attack is detected.

One famous cyberattack, highlighting the acute need for information sharing, is the "Great ATM Heist."[5] As part of this attack, a gang of hackers stole $45 million in two individual operations. Members of the gang succeeded in increasing the credit ceiling in bank accounts all over the world, and in making tens of thousands of cash withdrawals before being caught. The heist took place in two stages. During the first stage, on December 21, 2012, the hackers obtained information from five bank accounts, and increased the credit ceiling for those accounts. On the same day, field teams withdrew $5 million in cash from 4,500 ATM machines. During the second stage on December 19, 2013, the cyber thieves were more daring. This time, they obtained information about twelve bank accounts, and began a series of 36,000 withdrawals from ATM machines in New York and twenty-four other states in the United States and around the world, netting $40 million.

An important lesson in this case is the lack of cooperation between the agencies investigating the affair and between the parties at the banks responsible for preventing attacks and securing information assets. Law enforcement agencies were provided with details about the method of attack and the characteristics of the attack tools almost from the moment the first theft took place. Although they shared their analysis of the attack with the banks that had been attacked, due to a lack of effective sharing procedures, an overall picture of the situation did not emerge, and nobody

communicated relevant information to other financial institutions in a way that would enable them to prepare for similar attacks.

Together with the obvious advantages of information sharing, the drawbacks should also be noted, including the possibility that information-sharing mechanisms are liable to help the attackers and also provide useful information for new attackers, in addition to other risks that exist as part of the information-sharing process.[6] Nevertheless, the consensus among content experts is that the advantages of information sharing outweigh the disadvantages and risks, and that wise use of information-sharing mechanisms will enhance overall cybernetic resilience.

The aim of this article is to focus on the challenges and complexities facing information-sharing initiatives operating in the intra-sectorial sphere; analyze successful examples of intra-sectorial cooperation from other content areas; and finally provide recommendations for increasing the effectiveness of information-sharing initiatives in the intra-sectorial sphere.

The Sharing Space

In an ideal situation, companies whose databases are hacked – whether for criminal, espionage, or political objectives – will undertake a number of measures during the recovery process so that they can return to their routine functioning. First and foremost, they will contact law enforcement agencies and ask them to investigate the attack and prosecute the perpetrators. They will also inform their clients in order to jointly monitor actions and assess the effects of the attack in order to reduce the likelihood that it will spread, in addition to their duty to report the incident to the authorities, consumers, suppliers, and so forth. This is especially critical in the event of hacking of databases containing users' particulars. In cases in which the company attacked is a public one, the details of the attack will also be reported to the relevant securities authority and to the general public so that investors can make decisions about their investments in the company. Finally, the company will share information about the attack with other companies in the same sector,[7] which are likely to be exposed to the same threat. This information sharing should take place through a sectorial information-sharing center, which will receive the data, draw up a status report, and pass on the relevant details of the attack to the other companies in the sector, while simultaneously giving relevant information to inter-sectorial sharing agencies, such as national situation rooms.[8] For sharing to be effective and comprehensive, it must be focused and solidly based,

and it must take place in the **inter-sectorial** area – that is, among entities belonging to different sectors – and in the **intra-sectorial** area, among entities belonging to the same sector.

Every year, on April 7, the hacker organization "Anonymous" attacks entities identified as Israeli, labelled as an OpIsrael# attack. Preparation for this attack requires inter-sectorial information sharing among different sectors (media, health, transportation, financial, energy, and so forth). As part of this information sharing, state agencies, such as the national situation room, the Israel Security Agency, and the National Cyber Bureau convey information to all the relevant sectors in the Israeli economy. In some cases, the information is conveyed to sectorial cybernetic centers, which are currently being created in Israel, such as those of the energy and banking sectors.[9]

Intra-sectorial information sharing is also of great importance. Many investigations of cyberattacks indicate that the methods of operation, exploitation of breaches and weaknesses, and even phishing attacks typically spread throughout a single sector. Investigations of the modes of operation of criminal groups in cyberspace show that they are very active in gathering preliminary information on a sectorial level.[10] Furthermore, the malware development industry is characterized by specialization, sometimes based on sectorial systems. One such group is the Lizard Squad hacker group,[11] which focuses on developing malware specifically for gaming websites and attacking them.

Intra-sectorial sharing should be based on a model in which a group of information producers and consumers share information with each other. Instead of sending it directly to each other, however, the information is sent to a central administration, which then disseminates it to all the other consumers. This information is shared on the basis of its relevance for each sector – for example, information about a tool that attacks an existing weakness in a system that is widely used in a specific sector. Indeed, the sharing center serves as a clearing house for information for various organizations that serve as both producers and consumers of information.

One example that highlights the need for simultaneous, two-dimensional intra-sectorial and inter-sectorial information sharing is among developers and vendors of cyber defense technologies who share information with their colleagues in the sector in order to maintain a database of threats and weaknesses that is up-to-date, relevant, and precise as possible for all cyberspace users. This is in addition to the inter-sectorial sharing of

information with law enforcement agencies and state authorities in order to assist in the battle against cybercrime.[12]

The following is a schematic description of the information-sharing space:

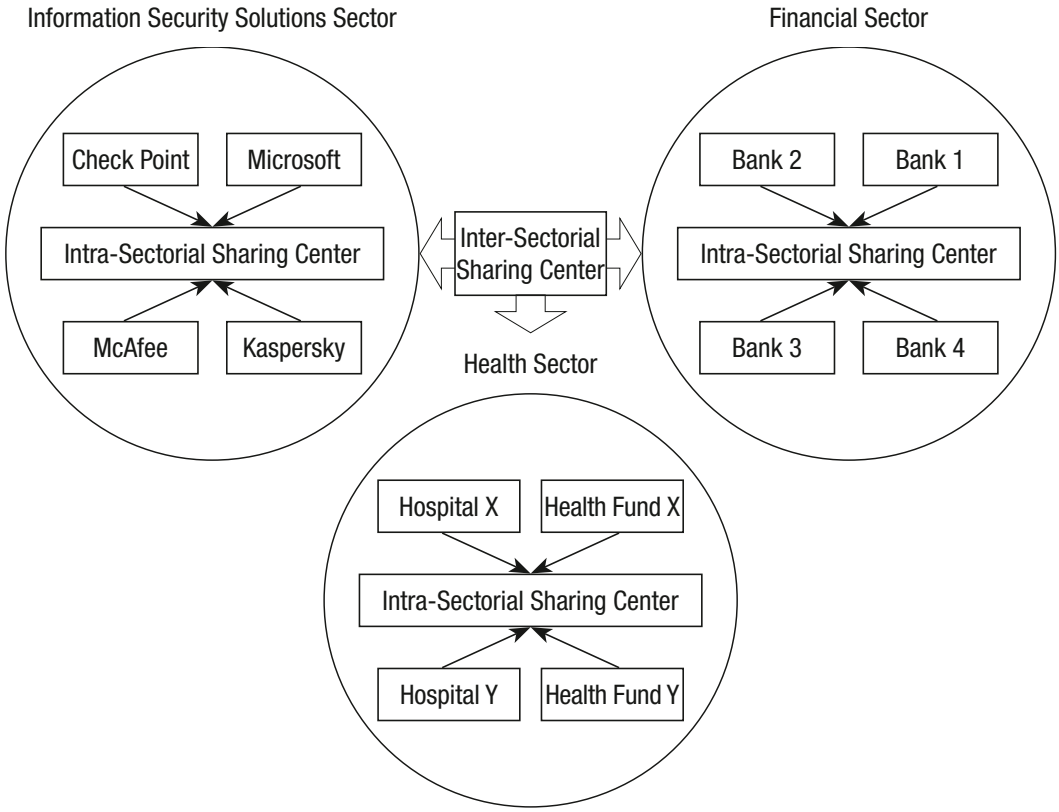

Figure 1: The Information-Sharing Landscape

Information-Sharing Challenges within the Same Sector

Even though information sharing has become a frequently-used term with a clear purpose among those working in cyberspace security, actual information sharing is only partial. Not many entities actively share information, while the volume of shared information and its relevance do not meet the needs of a given sector.

A study that examined the incentives and obstacles to sharing information about cyber threats found that the obstacles included economic ones, resulting from economizing, and concerns for the quality of the shared information, its value, and its use.[13] Concerns about receiving information of poor quality, exposing information security incidents that are liable to affect an entity's reputation, and poor management in information-sharing enterprises were the main impediments. It also emerged that companies

and organizations are reluctant to share information, out of fear that the information could prove useful to their competitors,[14] or that information sharing could harm a company's public image, by giving the impression that it is unable to protect its assets, leading to a drop in its sales and value.[15] Another impediment is what economists call the "free rider problem"[16] – a situation in which there is a lack of reciprocity; that is, competitors use the information received for their benefit, but do not contribute their own information to benefit others.

Most of the studies describe impediments to information sharing that are common to the specific sectorial environments of the companies and organizations. If they were not operating in the same sector environment, it would be reasonable to assume that these impediments would not have any impact. In fact, it can be concluded that that one of the significant factors hindering the development of successful information-sharing enterprises is the competitive factor. Organizations operating in a competitive environment find it difficult to launch information-sharing enterprises, even though it is clear to them that such sharing is useful to all the participants.

Competition and Cooperation – The Theoretical Background

Competition and cooperation are ostensibly two fundamentally opposite principles. The question, therefore, is whether they can exist together. Under conditions of competition without cooperation, the individual interest takes precedence over the group interest. On the other hand, when those cooperating rely entirely on their partners, a state of inefficiency prevails. It is therefore essential to find a point of equilibrium at which a certain level of cooperation occurs between the organizations active in the same sector and that is useful to all. Later, it is important to invest efforts in creating a solid basis for cooperation, so that competition and cooperation complement each other and coexist simultaneously.

Cooperation between competing entities will work in practice, and will improve their defense only if it includes a combination of competition and cooperation in a way that provides advantages to all the participants in the long term. Brandenburger and Nalebuff introduced the concept of "co-opetition" in a book they wrote in 1996.[17] They define co-opetition as a business strategy consisting of both cooperation and competition, aimed at achieving cooperation between competitors in order to obtain advantages that cannot be acquired any other way.

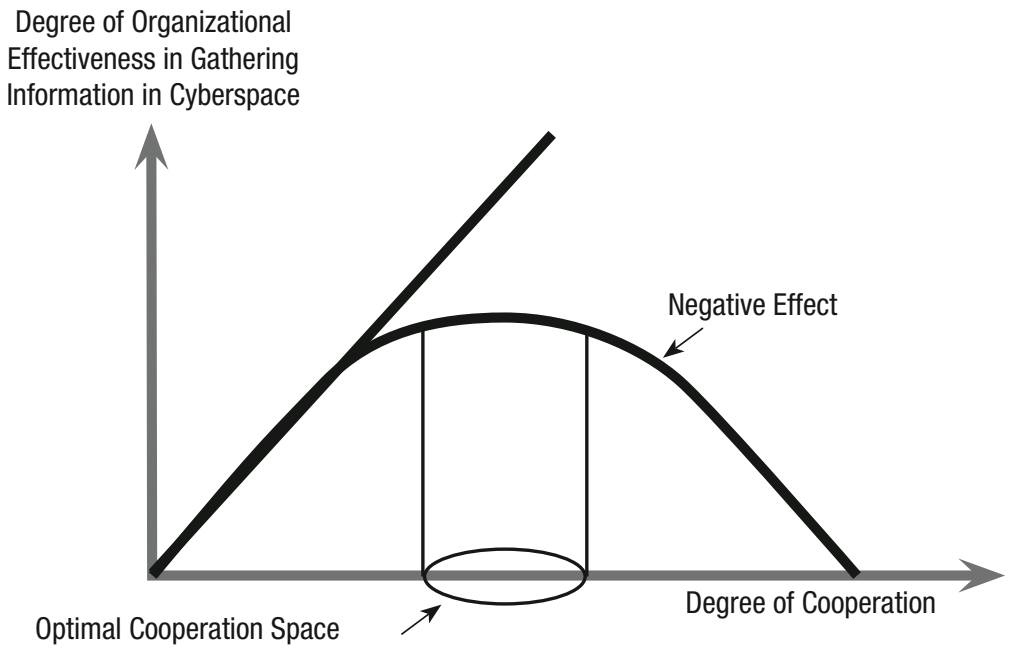

Figure 2: Point of Equilibrium in Cooperation

According to the co-opetition strategy, in order to obtain more business opportunities and increase profits, it is preferable to increase the total number of shared opportunities with competitors through cooperation, rather than making endless efforts to be better than them; in the context of cyberspace security, cooperation has great value. One example of co-opetition can be found in the challenging competition between the South Korean company Samsung and the Japanese company Sony; the two giant companies significantly improved their innovation processes and also encouraged small manufacturers to take part in the process and promote shared intra-sectorial interests.[18] On the other hand, some companies working in development believe that there is no room for cooperation based on an exchange of information. This thinking usually reflects their concerns that competing organizations will steal their ideas, or that cooperation will cause the competitors to produce better products.

Finding a balance requires analysis of the success factors in other sectors where structural processes of cooperation have been adopted, despite competitiveness and careful guarding of intellectual property. One example of a successful cooperative sectorial enterprise is in banking. In the early days of ATM machines in Israel, a customer could withdraw cash only from the banking network to which he belonged, and only from machines located within that network's branches. For example, a Bank

Hapoalim customer could not withdraw cash from a Bank Leumi machine. A few years later, the Automated Banking Services (ABS) company was founded and placed ATM machines in public places, serving customers of all banks. At a later stage, the banks agreed to improve their service by allowing every customer to use all of their ATM machines in Israel. In the past, ABS also considered establishing a cyber center for the financial sector in Israel, and submitted a request for this purpose to the director general of the Antitrust Authority, who was asked to assess the matter in the context of antitrust regulations in Israel. Recently it was decided to establish the financial cyber center as part of the national Cyber Event Readiness Team (CERT). One of the challenges facing the new center will be eliminating the "free-rider problem," – that is, finding a balance between the banks that will ensure continued optimal information gathering and sharing.

Another example of sector-wide cooperation can be found in the pharmaceutical industry. This industry regards cooperation as essential, and it shares information through a third entity that mediates between information requests and research. Many drugs were developed on the basis of research conducted in an open-source environment. One example is an enterprise formed in 2010 in which major drug companies, entrepreneurs, and research institutes combined forces in order to promote research methods for the development of drugs for two common mental illnesses.[19] This enterprise was created with the understanding that despite the enormous progress of knowledge in molecular biology and the prodigious efforts of all the parties engaging in drug development, the pace of developing new drugs had slowed; this was most likely due to the intensifying competition between rival drug companies on the one hand and the limited scope of information exchanges between academic institutions and the industry on the other.

The world of information technology can learn from cooperation between competing technological companies that have joined forces in order to establish standards for products and new technologies. For example, establishing standards for various detachable information-storage devices, such as video, DVD, and so forth, is a regular area of both cooperation and competition between Sony, Philips, Kodak, and many other companies.

Cyber-Information Sharing in a Competitive Environment

Two principal motives for competition between organizations in the context of cyber security and the players operating in the information-sharing sphere can be discerned: economic competition and competition for credit.

Economic Competition

Economic competition results in difficulties in cooperating, due to desires to achieve commercial supremacy and to increase the market share. This type of competition exists mainly among profit-driven organizations. In the context of cyber security, this type of competition can be found among companies that develop cyber defense products and services, such as anti-virus producers, firewall producers, managed security-service providers (MSSPs), and so forth.[20]

The purpose of information sharing between companies that provide cyber-security services is to create an optimal sharing infrastructure that will enable every threat discovered in one company's products to result in the updating of all the companies' security solutions, thereby improving the overall protection for cyber-security consumers. In order to bring about such information sharing, these companies must realize that despite the element of competition, cooperation between them is worthwhile. One especially difficult challenge is with the group of producers whose main business is cyber security.

From a commercial standpoint, companies that develop defense products understand that the databases on which their various products rely (such as the digital signatures of malware) are the raw material at the core of their systems. A security engine, however sophisticated, will not provide an appropriate and up-to-date solution if it relies on partial or irrelevant data. The reliability and current validity of the data are therefore among the most important factors in the quality of the systems and a key factor in their commercial success. Under conditions of competition, conveying information across-the-board among the producers of the various technologies is very difficult to achieve, especially among companies for whom this information constitutes the basis of the competition between them. Cooperation between MSSPs is also very limited. This sharing takes place only occasionally, and there are no structured mechanisms or processes for keeping the data up to date.

We are now witnessing a number of information-sharing initiatives in the cyber-security technologies sector. These enterprises are operating

simultaneously, and the companies that promote the enterprises have called upon others in the sector to join them. This has created a situation in which various companies within the cyber-security technology sector try to promote solutions to a problem; in doing so, they aggravate one of the greatest obstacles to finding a solution, and in effect, contravene the basic principle for which the enterprises were founded – cooperation for the purpose of creating added value. An example of this can be seen in the announcement in October 2014 of the establishment of the Cyber Threat Alliance enterprise by the companies of Fortinet, Palo Alto Networks, Symantec, and Intel Security, all which deal with cyber security technologies, while Microsoft is also promoting a similar initiative called VIA.

For information sharing to be effective in the way that the companies convey and receive the information when it is still "hot and relevant," it must be based on automated information-sharing solutions. A number of standardization activities are taking place in this area, supported by the US Department of Defense, under a shell architecture called CyBOX.

Competition for Credit

This competition stems from the difficulty of sharing information, resulting from the desire for professional esteem and a good reputation; the idea that knowledge is power; and an inter-organizational culture sometimes characterized by power struggles. This type of competition is also found among countries; agencies working to promote and improve the level of national cyber security; and non-profit entities, such as research institutes and academic institutions.[21] The advocates of inter-organizational coordination and integrative plans assert that the problems facing a country are complicated, and dealing with them therefore requires an integrated approach. They recognize the fact that coordination can create economies of scale, and that a measure taken by a number of organizations is more powerful and effective. Nevertheless, multiple plans and the overlap between them requires great coordination, which complicates information sharing and detracts from its effectiveness.

One of the models,[22] which examined ways of dealing with obstacles within the framework of cooperation between state agencies, raised a number of points that require attention in order to overcome these impediments:

1. **Sovereignty**: An organization customarily regards itself as a sovereign entity within its content world and within its authority. A state organization will therefore cooperate only if it directly contributes to the

organization's objectives and goals. Even in cases in which cooperation is backed by a binding policy, a certain degree of voluntary participation is needed. People consider first and foremost the direct contribution that cooperation will provide for their organization before they will consider cooperative efforts that will benefit others.

2. **Complexity of cooperation**: Defining processes of information sharing is complicated, and includes a certain degree of uncertainty about the right way to proceed. It is important to address this aspect in the process-outlining stage by adding monitoring and feasibility tests.
3. **The dimension of size**: Smaller organizations are likely to perceive cooperation with larger organizations with ample budgets as threatening and non-voluntary. This lack of balance leads to opposition in the coordination processes.
4. **Organizational culture and work methods**: Every organization has its own unique organizational culture, including planning methods, monitoring, and timetables. Each organization tends to regard their own work methods as the best and most suitable.
5. **Communication and language gaps**: Every organization has its own patterns of communication and unique terminologies. It is important to define a common language that all the partners can understand.
6. **Asymmetry of the participants**: Assuming that the participants are not equal in strength and size, they should be asked what volume and quality of information they will be able to supply, compared to the volume and quality of the information received.
7. **Instability and uncertainty**: Cyberspace is characterized by many risks. Thus, sharing technological tools that contain elements of a company's intellectual property could expose the information to undesirable parties.
8. **Incentives for sharing**: Cooperation through an agency responsible for coordination will not solve all the problems and obstacles encountered. It is important to devise incentives that will encourage all the partners to contribute to the joint effort.

One fruitful example of information sharing can be seen in the activity of a forum called Intellipedia, which was founded after the terrorist attack on the United States in September 2001. As a result of the attack, decision makers in the American security services realized that the idea of each agency developing and managing knowledge by itself did not contribute to national security; the intelligence information did not flow between the country's various security agencies, resulting in their inability to thwart the

attacks. The American security apparatus therefore established a joint forum facilitating information sharing between various organizations. Although here, too, we see competition for resources, sources of information, and prestige, the forum's success is based on the realization of the various organizations that information sharing can only benefit the public and enhance national security.

Since the beginning of the twenty-first century, initiatives for data-sharing centers have been operating in the United States in various sectors, such as health, finances, and so forth. These initiatives are called information sharing and analysis centers (ISAC), and they all operate according to similar principles. The National Council of ISACs (NCI) was formed with the objective to encourage intra-sectorial information sharing by formulating work principles and procedures, and to promote connections between the various centers. Member organizations share ownership of these enterprises, and receive technological and economic support from the US Department of Homeland Security.

Companies operating in the same sector naturally compete with each other, but they cooperate in this area because cyberspace is not the essence of their business. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) focuses on information sharing in the financial sector in the United States. This center operates according to the following operative principles: the organization belongs to its members, is managed by them, and maintains databases containing information about cyberattacks, physical security attacks, threats, weak points, and solutions. The information is gathered from both the organization's members and external parties, such as government security agencies and other ISACs. There are several levels of membership in a center, and payment is determined according to level of service: a higher level of membership means the organization receives more services and is exposed to more information. In the operational aspect, information can be conveyed to the FS-ISAC either anonymously or openly. The information is checked by a team operating around the clock, which analyzes and classifies the data, and conveys the information to the members in accordance with the principles.

A study conducted following a number of serious cyberattacks in the financial sector and among the FS-ISAC member organizations examined alternative models for promoting and improving information sharing from both a quantitative and a qualitative perspective.[23] The study included the

use of game theory tools, which were used to examine the existing models for payment of membership fees in ISACs and their effect on the level of sharing. The research showed that most of the existing models in ISACs create an imbalance between the high expectations of the members to obtain information and their reluctance to share information, and is inconsistent with the declaration of intent made by each member upon joining the ISAC.

The study also considered an innovative theoretical model based on the idea that payment for membership in ISAC can be used as an insurance policy providing coverage for damage caused by a cyberattack, in contrast to the accepted models based on payment of membership fees according to the level of use. The developers of the new model showed that when payment for membership in ISAC is based on levels determined by the extent of use, the member organizations do not have any incentive to share information about cyber incidents with their colleagues. In contrast, when the model is based on paying a premium according to the size of the expected loss for all the organizations, and for which in exchange they receive an insurance policy funded from a general pool of premiums, the members show an interest in information sharing; each organization is safer when all the other organizations are more secure.

Recommendations

Given the above analysis, and based upon the assumption that intra-sectorial information sharing is extremely important to improving the overall defense of a sector, several recommendations can be made to assist in the successful establishment of cyber-information-sharing initiatives in a single sector environment:

1. **Mapping of partners**: At the stage of initiating, developing the idea, and understanding the expected results, potential partners should be mapped, and thought should be given to the desired composition of the partners. At this stage, initial exploration of potential partners should be conducted, and each party should consider whether it is willing in principle to join the partnership. It is best to define as precisely as possible the results that the sharing enterprise seeks to achieve and the tools at its disposal, including technological, regulatory, economic, public relations, and other capabilities.
2. **Cost-benefit ratio**: Organizations are not eager to share information at any price. Successful information sharing requires that the benefit for each party outweighs the time and costs involved in the partnership. In

certain cases, incentives should be considered to encourage support for information sharing. It is important that organizations recognize and understand the quantitative advantage and economic value of successful sharing. This method has been found to be effective in creating an incentive for sharing processes, as well as within the context of securing the budget for the information-sharing enterprise. The budget should be determined in the initial stages of the enterprise, so that it will be clear to all the partners who is bearing the costs of the plan.

3. **Types of partners**: It is recommended to define the partners for the enterprise. A distinction should be made between three types of partners – interested parties, owners of information, and parties that have authority – as well as an assessment of their importance and contribution to making the enterprise more effective. Every partner has a unique perspective. In order to increase trust among the partners, communications between them should be structured, and a common language created. It is important to create a "shared experience," and to devise routine operations, which should be agreed upon in the planning stages of stage of the enterprise.
4. **Commitment and authority**: All the partners should give a minimum commitment at every stage, from the initiating and planning stage to the implementation and periodic assessment of the plan's effectiveness. A number of key questions concerning the authority to make decisions, leadership of the entire process, and timetables need to be considered, as well as who should be included, when they should be included, and how it should be done. The partnership's success depends on each partner knowing in advance what they are expected to contribute to the process and what they will receive in return. The sphere of action and areas of responsibility should be determined for each partner, and the interdependence between the partners should be stressed. It is recommended to announce the leading party that has authority and responsibility for the process and its results in the early planning stage. Two types of leadership can be specified: professional, led by the most relevant responsible and professional partner, and operational, led by a partner with methodological expertise in managing cooperative processes, and who is perceived as being free of any personal interests. An individual committed to the common goals should be appointed to head the project.

5. **Ego and prestige**: Dealing with ego and prestige requires advance preparation. Instead of assuming that ego does not play a role, and that everyone acts according to professional considerations, it would be better to assume the opposite. The uniqueness of the players should be emphasized, and the ego regarded as a professional value that each entity brings to the information-sharing plan. It is important to recognize the limits of responsibility of every organization, and to give space to each organization's accumulated experience and knowledge,
6. **A decision-making mechanism**: Solving disputes requires a mechanism for making decisions within the framework of the partnership. The decision-making mechanism in situations of conflicts already should be defined in the planning stage. It is important to recognize that when dealing with disputes, it is essential to clarify them and reach agreement among the partners about the nature of the dispute. Discussion and dialogue need to be thorough before a decision can be made, and a large degree of transparency should be encouraged.
7. **Monitoring**: Monitoring and assessment mechanisms are critical for success. Monitoring should take place through orderly mechanisms anchored in joint activity, upon achieving periodic targets and measures. These targets and measures should be taken into consideration during the implementation stage, and they will assist in making correct data-based decisions, preferably by an objective external agency. Based on the summary assessment, a decision can be made regarding the extent of implementing the plan, and whether it needs innovations and changes. It is important also to periodically evaluate the external changes that are likely to affect the effectiveness of the enterprise, such as regulatory and technological changes.
8. **Cooperation at the national level**: Public agencies at the national level, such as national CERTs and other government institutes, should be encouraged to share information with each other. It is important that these agencies are active in promoting cooperation and developing platforms that will provide solutions to the various obstacles that impede information sharing. A training program should be devised for creating, developing, and maintaining the skill and expertise necessary for operating information-sharing centers. At the same time, it is crucial to find a balance between state involvement in managing and carrying out sharing processes and the need of certain sectors to protect the shared information, due to its nature and sensitivity. There are some

sectors (e.g., the insurance sector) whose information is highly sensitive to privacy. In such cases, the state should allow independence in information sharing, with minimum intervention.

At the operative level of planning an information-sharing enterprise, it should be verified that the information is relevant to the partners, of appropriate quality, and timely. Forums should be held for this purpose, with the aim of defining all aspects of the sharing process. For example, sharing information about the Internet Protocol (IP) of a specific attacker is essential. At the same time, other unique attack characteristics should not be shared with others, in order to prevent misuse of the information shared.

Conclusion

Information sharing in the field of cyberspace is very important, as the information critical to coping with cyber threats is dispersed across countries and organizations all over the world. Information sharing can include reciprocal briefings about attacks (methods, means, targets); weaknesses; and methods for dealing with specific and general threats. Sharing of optimal information makes it possible to present an up-to-date and relevant picture of cyber threats at the sectorial, national, and global levels. Information sharing also lends support to decisions to invest in appropriate and relevant resources against the developing threats. Finally, successful information sharing also assists processes of research and development of solutions designed to counter cyber threats.

Currently many information-sharing initiatives are managed as state, sectorial, or private initiatives. One of the leading and most significant mechanisms is the information that security and defense companies provide to their clients – information that usually originates with the company's clients who have been attacked. The assumption is that this mechanism operates optimally. Another information-sharing mechanism regarded as highly effective, although not ideal, can be found in the sectorial CERTs. Many organizations are intuitively, informally, and only partially setting up information-sharing mechanisms. It is important to establish a global enterprise that will operate according to the operational principles of the information-sharing enterprise of the security companies. All the information gathered in the framework of a global enterprise will be cross-referenced and analyzed, as is done by the security companies' enterprise, and the processed information will then be sent back to all the clients of all the partners.

Despite the many obstacles that must be overcome in order to operate information-sharing initiatives, the establishment of CERTs is critical for improving general security in cyberspace. It is therefore appropriate for the mechanisms proposed here to be included as part of the "toolbox" for initiating, designing, and operating such centers.

Notes

1 This refers to weak points, sometimes identified and known, and usually resulting from faulty design, which an attacker is able to exploit in order to penetrate a system or disrupt its operation.

2 Experts on information sharing in cyberspace frequently have clamed that information sharing is risky, in that the information is liable to be revealed to the general public, thereby helping the attackers while also providing useful information to new attackers, in addition to other risks incurred in the process. For a thorough review of this subject, see ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, (ENISA, 2010).

3 This is a broad concept that relates to the endurance and strength of cyberspace when facing the threats and risks liable to disrupt its activity or the way it is used.

4 Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affairs*, May 7, 2015.

5 Marc Santora, "In Hours Thieves Took $45 Million in A.T.M. Scheme," *New York Times*, May 9, 2013, http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?_r=1.

6 As noted above, a full review of the advantages and risks can be found in ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*.

7 A sector is a group of entities in the economy sharing similar characteristics, operating in a similar business environment, and having similar objectives, such as the "business sector."

8 National war rooms exist in many countries around the world. Their purpose is to assemble a national status report in cyberspace and coordinate information sharing between sectors and between state agencies and civilian entities.

9 Ami Rojkes Dombe, "Meet the Cyber Center for Energy in Israel," *Israel Defense*, November 25, 2015.

10 Lillian Ablon, Martin C. Libicki, and Andrea Golay, *Markets for Cybercrime Tools and Stolen Data*, (National Security Research Division, Rand Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

11 Jimmy Blake and Amelia Butterly, "Who are Lizard Squad and What's Next for the Hackers?" *BBC*, January 27 2015, http://www.bbc.co.uk/newsbeat/article/30306319/who-are-lizard-squad-and-whats-next-for-the-hackers.

12 For a broad survey review covering the entities and initiatives promoting the sharing of cyberspace information, see Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing," *Military and Strategic Affairs* 6, no. 3 (December 2014): 59-77.

13 ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*.

14 Andrew Nolan, *Cybersecurity and Information Sharing Legal Challenges and Solutions* (Congressional Research Service, March 16, 2015), https://www.fas.org/sgp/crs/intel/R43941.pdf.

15 Maria Cristina Arcuri, Marina Brogi, and Gino Gandolfi, "The Effect of Information Security Breaches on Stock Returns," Università di Roma La Sapienza, 2014.

16 Russell Hardin, "The Free Rider Problem," *The Stanford Encyclopedia of Philosophy*, Spring 2013.

17 Adam M. Brandenburger and Barry J. Nalebuff, *Co-opetition* (New York: Doubleday, 1996).

18 Devi R. Gnyawali and Byung-Jin Park, "Co-opetition between Giants: Collaboration with Competitors for Technological Innovation," *Research Policy* 40, no. 5 (June 2011):650-663.

19 "Prof. Jonathan Rabinowitz from Bar Ilan University is one of the leaders of an international project to bring about a breakthrough in the development of a drug for common mental illnesses," Bar Ilan News, Spokesperson's Office, Bar Ilan University, December 7, 2010.

20 This consists of continuous monitoring services for information security systems and analysis and adjustments between data for early and proactive detection of threats. This analysis is conducted by cross referencing all the data obtained from all of the company's clients and sending the relevant information back to the companies.

21 In certain cases, this sector also features economic competition.

22 Susanna P. Campbell and Michael Hartnett, *A Framework for Improved Coordination: Lessons Learned from the International Development, Peacekeeping Peacebuilding, Humanitarian and Conflict Resolution Communities*, October 31, 2005, https://www.regjeringen.no/globalassets/upload/ud/vedlegg/missions/framework.pdf.

23 Charles Zhechao Liu, Humayun Zafar and Yoris A. Au, "Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector," *Communications of the Association for Information Systems* 34 (2014).