Extract from a research paper "Enhancing cyber security in Poland through effective public and private sectors cooperation." prepared at the George C. Marshall European Center for Security Studies in 2016. The view expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the Polish Government, the Ministry of Digital Affairs, or any of its agencies.

Agnieszka Wierzbicka

Introduction

Over the last ten years, Information and Communications Technologies (ICTs), including the Internet, have become essential to the functioning of the economy as well as a key driver for development in all sectors. Governments, public and private organizations as well as individuals have become dependent on the digital environment for their core activities. However, they are facing a growing number of uncertainties related to the use of the digital environment. Cyber, digital and ICT hardware security threats and incidents have increased, leading to significant financial, privacy, and reputational consequences, and in some cases even to physical damages. Digital security incidents can have far-reaching economic consequences for organizations. Examples of such economic consequences include disruption of operations (e.g. through denial of service attacks, disruption of information assurance and sabotage), direct financial loss of hundreds of billions of euros each year[1], lawsuits, reputational damage, theft of intellectual property, technology, research, loss of competitiveness (e.g. in case of theft of trade secrets), as well as loss of trust among citizens, customers, employees, shareholders and partners.

It is often said that information is power, and this is a key service that Public-Private Partnerships (PPP) provide. This concept is particularly true in a world that moves at the speed of light, *Internet speed*. Timely, accurate and expeditious sharing of cyber security-related information between organizations – in a critical sector, cross-sector, nationally and internationally – is widely perceived as a vital measure for effectively addressing the cyber security challenges of organizations. One of the key outputs of this mode of information sharing is the establishment and trust-building between people and organizations. Information sharing is an effective approach for managing the collaborative cyber risk in a domain where the threat landscape is continuously changing. The sharing or exchange of information is increasingly being encouraged by legislators and other stakeholders who

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime (2014)*. Center for Strategic and International Studies, 2014. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed August 19, 2016).

recognize that the ability to reduce cybersecurity risks to government systems, critical infrastructures, and enterprises increasingly depends on this form of proactive collaboration. However, the security benefits of sharing information must be achieved in a way that does not erode privacy or adversely impact individual freedoms and rights. Strong privacy and civil liberties protections are paramount if an information sharing program is to be widely accepted and successful. No organization can address the full spectrum of its cyber security and resilience on its own, as organizations are trending toward global interconnectedness, and are consequently exposed to the same global cyber security threats. Collaboration with partners across organizational, functional/sectoral, and national boundaries, and from small and medium enterprises up to multinationals private enterprises and governments is therefore required. This is essential in order to counter dynamic and multidisciplinary cyber security threats which may negatively impact the organization and its services. Moreover, in most cases Critical Infrastructure (CI) is privately owned and operated. The private sector holds considerable expertise in the development of internet policy, creation of cyber technology, and defense against network intrusions.

PPPs are one of the forms that public and private sector use to share information about incidents, vulnerabilities, threats, strategic related topics, operational methods and best practices. A number of countries[2] have gained substantial experience with PPPs, where they have brought together key stakeholders, including government, national agencies, regulators, IT companies, IT security firms, business enterprises, and private critical infrastructure and security researches. This cooperation has evolved disparately, depending on the environment, culture and legal framework of a given country. Some of these PPP have been legislatively or regulatory mandated. Others have developed by like-minded organizations of their own accord.

Keys to success of effective Public Private Partnership

The creation of trust is vital for the success of any PPP, as the information shared within PPP is often sensitive. It is essential to create an atmosphere of trust in which both public and private parties show awareness of each other's need for discretion, and consistently act accordingly. Building trust is especially important when the initiatives are based on voluntary information sharing and membership. As a primary characteristic of trust-reliant

[2] Such as Germany, Great Britain, Netherlands and United States.

PPPs, it should be clear to all partners of a particular PPP that the goal of cooperation does not aim to reveal stakeholder weaknesses or gaps in terms of cyber security. Effective PPPs create a climate of confidence and trust, in order to share good and bad practices between applicable stakeholders, exchange experiences around events, discuss preparedness measures and even reactions from citizens or regulators in the broad subject area of information security. Trust is built among participants based on their contributions, collective actions, and shared experiences. There are various methods for building trust, such as informal meetings, small group meetings, transparency, teleconferences, networks of trust and reputation-based trust anonymously established by voting - Information Sharing and Analysis Centre (ISAC) or Information Sharing and Analysis Organization (ISAO[3]) and use of Traffic Light Protocol[4] and of other[5] standards establishing some rules on how information should be communicated. Within a framework of trust-building, significant value is assigned to creating an atmosphere of partnership from the outset. This can be achieved by reaching out to stakeholders early on, ideally at the "blank page" stage and by an involvement of public and private sector partners at the priority/goal and objective phases of projects and not only by an implementation. Continuous and regular interaction between stakeholders is needed, in order to foster cooperation. Trust is also built by establishing co-leadership of programs and consensus partnership decision making. Secondly, an effective PPP can be characterized by a clear set of rules that regulate the PPP framework, such as a Memorandum of Understanding, or – in the case of larger membership – a (Cyber) Information Sharing Agreement (or at a minimum, developed guidelines and etiquette to meet in a structured and useful way). The rules should prevent any conflict of interest and reduce ambiguity, indicate clear lines of responsibility and accountability, and set down achievable goal and establish incentives for partners. Another key to success is clear common interest that establishes a basis for co-operation and creates a win-win situation for all participants. There has to be a balance between a private sector (which regards cyber-security challenges as financial and a matter of reputation), and the public sector (where cyber security is viewed as a common public good).

[3] Currently, most private sector information sharing is conducted through ISACs. ISACs operate through a sector based model, meaning that organizations within a certain sector (i.e. financial services, energy, aviation, etc.) join together to share information about cyber threats. Although many of these groups are already essential drivers of effective cybersecurity collaboration, some organizations do not fit neatly within an established sector or have unique needs. Those organizations that cannot join an ISAC but have a need for cyber threat information could benefit from membership in an ISAO.

[4] http://en.wikipedia.org/wiki/Traffic_Light_Protocol (accessed August 19, 2016).

[5] ISO/IEC 27010. *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*. ISO, Geneva, 2015.
http://www.iso27001security.com/html/27010.html (accessed August 19, 2016).

To avoid misunderstandings and mistakes, clarity about tensions and competing agendas are needed. If the interest of the partners are not well aligned, governance by rules is advised. An awareness of each other's priorities, goals and limitations is necessary. This prevents conflict through misjudgment of the cause of a negative response and allows for an optimum return on the efforts of the PPP. This implies that both public and private parties should know each other's (business) drivers and evaluate whether the objectives are still clear, and that PPP activities align with these objectives. Collaboration is only feasible if both sides understand each other's objectives, their mandate and standard operating procedures. Moreover, top management of the organization needs to have a clear view of the objectives of these activities and how it is beneficial to the business objectives of the organization in areas such as the protection of shareholder interests.

A significant benefit from PPP is the sharing of information. It is crucial to provide equal value in-kind to the information received, within an appropriate timeframe which encourages each participant to cooperate and increase trust in the organization or initiative. A secondary and equally important benefit is individual personal network enhancement and building. Through such information-sharing, a gradual elevated level of mutual trust and further information-sharing can be fashioned. To begin collaboration and information-sharing requires momentum. Energetic engagement by each of the participating organizations helps ensure momentum with continuously increasing added-value to all stakeholders. Senior level commitment of public and private sector partners to the partnership process should be communicated to staff and upper echelons. A good practice is also to make use of existing initiatives.

PPP works best when the collaborating organizations operate at much the same cyber security maturity level. The maturity of the organization is displayed by its willingness to share sensitive cyber security-related information, the professionalism and experience of its cyber security staff and organization, and the ability to professionally and securely handle sensitive information received from other organizations. In contrast to the preference for organizations of comparable capabilities or equal 'cyber maturity,' in some communities not all organizations are equally capable or as 'mature' as others. Larger organizations still may benefit from investing in information-sharing and protection of smaller ones, as such reassurances positively impact the sector's image overall. Organizations have different backgrounds and ways of operating, especially if it concerns organizations in an international

context. The differences stem from a mixture of perspectives such as: public or private, more or less cooperatively minded, culture, national history, organization's history, language, judicial system, political and ethical differences, as well as experience, norms, procedures, processes and practices.

Language differences stem from translation between, for example, English and German, and from different vocabulary such as technical terms ("sector-specific slang"). Insufficient attention to such differences on the edges of interaction between people, technology and processes may hamper collaboration and information sharing. Involving individuals who can cross cultural barriers as facilitators (and not their 'bosses' who might not be able to function in such a capacity), may help to stimulate the information flow between diverse communities. Moreover, organizations should not be pressed to share information against their unique specific desires. If required to do so, they might potentially shift to demonstrating a reluctance to share as a negative outcome, for example by overloading the recipient with low value information. However, in some instances, (such as in the case of national security and public safety), there may be a need for mandatory incident reporting. The debate between mandatory and voluntary information sharing is an ongoing hot topic. The keys to a successful PPP listed above are certainly not an exhaustive list of factors needed for the establishment or maintenance of effective PPPs, but they point out characteristics worthy of consideration that were identified by numerous research studies[6].

---

[6] Clinton Larry, *Best Practices for Operating Government – Industry Partnerships in Cyber Security*. Journal on Strategic Security 8, no. 4, 2015, 53-68.
http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1456&context=jss&sei-redir=1&referer=http%3A%2F%2Fwww.bing.com%2Fsearch%3Fq%3D%25E2%2580%25A2%2509Larry%2BClinton%2B%282015%29%2C%2B%25E2%2580%259CBest%2BPractices%2Bfor%2BOperating%2BGovernment%2B%25E2%2580%2593%2BIndustry%2BPartnerships%2Bin%2BCyber%2BSecurity%25E2%2580%259D%2C%26src%3DIE-TopResult%26FORM%3DIETR02%26conversationid%3D#search=%22%E2%80%A2%20Larry%20Clinton%20%282015%29%2C%20%E2%80%9CBest%20Practices%20Operating%20Government%20%E2%80%93%20Industry%20Partnerships%20Cyber%20Security%E2%80%9D%2C%22 (accessed August 19, 2016).
Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches. ENISA, December 2015. https://www.enisa.europa.eu/publications/cybersecurity-information-sharing (accessed August 19, 2016).
Bendiek Annegret, *Due Diligence in Cyberspace – Guidelines for International and European Cyber Policy and Cybersecurity and Cybersecurity Policy.* SWP Research Paper, May 7, 2016. https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf (accessed August 19, 2016).
Comparative Models for Effective Public Private Partnerships. Desktop research report. ENISA, 2011. https://www.enisa.europa.eu/publications/copy_of_desktop-reserach-on-public-private-partnerships/at_download/fullReport (accessed August 19, 2016).
Comparative Models for Effective Public Private Partnerships. Good Practice Guide. ENISA, 2011. https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps/at_download/fullReport (accessed August 19, 2016).

Challenges for PPP

There are many challenges for PPP that create obstacles to information sharing. It is sometimes contrary to private-sector commercial interests to report vulnerabilities, particularly if understanding and rectifying a problem before competitors become aware of it could offer a market edge. The public sector also encounters limitations to sharing information. Classified and sensitive information, as well as trade secrets, cannot be shared with individuals who do not have adequate security clearance. Even those working in the private sector who do have security clearance can often do nothing with classified information due to law and regulation. Further, there is a high expectation that threat information shared from the public to the private sector will be accurate, and this leads to extensive and stringent review and revision processes that delay the release of time-critical information. High turnover of staff in public sectors is a human factor obstacle, and often hinders effectiveness, especially regarding trust issues. Hesitation to share information may be also stem from the fact that passive and perhaps noncontributing members of PPPs are not penalized, or because the conditions to become member of certain initiatives are rather informal. What could be even more counter-productive for PPPs is lack of respect for the confidentiality and for the established rules of cooperation to which stakeholders of an initiative agreed to adhere. An efficient information exchange between organizations of different countries is also hindered by different national legislations and local regulations imposing data localization requirements, information storage restrictions, as well as information secrecy and non-disclosure rules.

Certain countries or sectors consider that information sharing on cyber incidents may ultimately be interpreted, on the grounds of the local or European regulation, as anti-competitive behavior and hence is likely to infringe on competition rules. Furthermore, law enforcement and other public officials may have multiple conflicting tasks and role

---

Luiijf Eric and Kernkamp Allard, *Sharing Cyber Security Information – Good practices stemming from the Dutch Public-Private-Participation Approach.* GCCS 2015, March 2015. https://www.thehaguesecuritydelta.com/media/com_hsd/report/40/document/Sharing-Cyber-Security-Information-GCCS-2015.pdf (accessed August 19, 2016).

Carr Madeline, *Public-private partnerships in national cyber-security strategies*. International Affairs 92: I, 2016. https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf (accessed August 19, 2016).

Goodwin C., Nicholas J.P., *A framework for cybersecurity information sharing and risk reduction*. Microsoft Corporation, USA. http://www.microsoft.com/en-us/download/confirmation.aspx?id=45516 (accessed August 19, 2016).

ambiguity. Sharing detailed threat information to enhance the common situational awareness may also, under certain legal frameworks, oblige a law enforcement official to change hats and use that information for investigation purposes. As a result, the source of the information may be leaked to court and or may damage the reputation of the affected organization(s). However, the biggest barriers in the information sharing process seem to be the national laws and regulations on personal data protection. For example, in several cases the national laws that consider IP addresses as personal data do not allow organizations to exchange this type of information, even if it could be helpful to other companies.

Recommendations:

- **Ensure whole-of-society community involvement within and surrounding both the public and private entities.** PPP should be informed by knowledge of the partners most appropriate to accomplish its professed goals. At the most basic level, both public and private sector entities have vested (though varying) interests in cybersecurity and must be engaged. Because leadership support at the highest levels is key to success, public sector engagement should include representatives from key ministries for cybersecurity. The engagement of state, local and territorial government entities across the nation is also important to ensure the security of critical digital infrastructure at the regional and local levels. International governments must be engaged too – either through inter-governmental channels or directly through PPPs – to ensure the interoperability of both technical and policy solutions. Finally, the sphere of appropriate private sector partners includes both industry and the nonprofit community, with the latter encompassing both academia and advocates for privacy and civil liberties. For example, the involvement of nonprofit organizations focused on Internet governance is imperative to achieving policy coordination, while those focused on technological advancement are vital to fostering research and development in the area of cybersecurity – as are the academic counterparts in either arena. It is equally important that private sector partners include industry entities of varying size, from the largest corporations to those still in startup mode. Further, while the support of senior leaders from each sector is vital, it is equally important that partnership extend to the tactical levels within partner organizations in order to ensure that the most nuanced engagement occurs between

experts at any rank. Thus, any partnership must allow for connection among senior officials, and between those working at a tactical level in various partner entities.

- **Speak with clarity about the tensions and competing agendas.** Government stakeholders appear to approach cybersecurity as a matter of national security, they require information and expertise from private sector entities in order to secure cyberspace effectively and thus, consider partnership a public good. In contrast, their private counterparts appear to view cybersecurity as a necessary expense in order to safeguard investments in intellectual property and other assets. Partnership with the public sector is of interest only to the extent that it furthers the goal of maximizing profit. By clearly establishing an end goal, partners can more easily overcome cultural differences, achieving success even while working toward it in very different manners.

- **Build trust that corresponds to a mutual belief in the positive gains of both partners.** Trust as the essential underlying element to successful relationships could be built only over time and, primarily, through personal relationships. PPPs should implement policies which maintain continuity of membership such as clear membership rules on participation, backed up by incentives. Having the 'right people' in the partnership is another way to develop trust. Members that are empowered to bring value that cannot be gained elsewhere will increase the motivation to build trusted relationships. In addition, trust must be built both ways, it means a recipient will not abuse the information nor cause harm to the source, but on the other hand there is a need for trust in the source so that the recipient can be confident that the information is accurate and not misleading. That is why PPPs should adopt information distribution policies such as the Traffic Light Protocol[7] to give the source confidence that the information will only be used as agreed. Moreover, in some cases to ensure trust it is necessary to include Non-Disclosure Agreements, and arrangements for sharing sensitive information.

[7] https://www.first.org/tlp/

- **Develop incentives on behalf of the public enterprise**. Thomas[8] and Clinton[9] stress in their study that, as much as trust building is vital in developing true partnership, incentives must also be properly aligned to reward each sector for their engagement. An incentive-based approach is best accomplished by tying incentives to results rather than activities. Incentives may include: reduced risk exposure by better security and resilience; cost savings from sharing the work to solve a critical problem, access to privileged Information from government, access to knowledge not available elsewhere, opportunity to avoid inappropriate regulation, opportunities to contribute to strategic direction and national policies; technical knowledge, intelligence, research and analysis, leverage the skills, experience and organizational positions of the existing members, revoking membership for not contributing/attending meeting.

- **Establish legal/regulatory framework.** Proliferation of PPPs focused on securing cyberspace over the past decade suggests that legislation is not necessary in order for public and private entities to work with one another in partnerships. However, legislation could help create a regulatory environment more conducive to voluntary partnership like in the financial or telecommunication sector. Measures clarifying the authority that various public institutions have to aid the private sector in the case of cyber intrusions would enable such public institutions to respond better to requests in a timely manner such that private entities are more likely to see value in partnership. The rules should prevent any conflict of interest and reduce ambiguity.

- **Design a bottom-up approach.** A partnership driven primarily by a need for accountability will require more rigid infrastructure (and perhaps a contractual network of sorts) whereas a partnership valuing flexibility will be better suited by a looser framework. Given that cybersecurity is a matter of national security, it might seem logical to value accountability above flexibility in the design of a related PPP. However, the fast-evolving nature of cyber threats, and the need for rapid technological advancement to address such challenges, makes flexibility extremely important in a cybersecurity PPP. This does not preclude regulatory mechanisms to encourage an environment in which partners are held accountable for their activities,

[8] Thomas Nyswander Rachel. *Securing Cyberspace through Public-Private Partnership. A Comparative Analysis of Partnership Models*. August 2013.
[9] See footnote 6.

but the structure of the PPP itself must be flexible enough to meet its objectives as cyberspace evolves.

- **Create a sound and sustainable financial package (UK case)**. Government can add value and reduce economic barriers to PPP participation by covering the costs of administration and venue.

- **Maximize transparency.** Clearly inform the participants of the relevance and real added-value of PPP as well as be transparent regarding the rules and practices followed.

- **Appropriate risk allocation and risk sharing.** Cyber security related issues need to be part of the permanent risk management cycle of an organization.

Way forward

Public-private partnership remains a vital and effective tool for achieving the national cybersecurity goals. However, the proliferation and evolution of cyber threats continues to outpace efforts to prevent, protect against, mitigate and recover from such attacks, making it evident that more must be done to secure cyberspace. In particular, resources must be focused on research and development, technical standard setting, national and international policy development, and the building of human capital if the Europe is to shift the balance in its favor.