PUBLIC-PRIVATE PARTNERSHIPS

PER CONCORDIAM ILLUSTRATION

BUILDING A STRONG FOUNDATION FOR PROTECTING VITAL SERVICES

By **Agnieszka Wierzbicka**, Department of Cyber Security at the Polish Ministry of Digital Affairs

Over the past 10 years, information and communications technologies (ICTs) have become essential to the functioning of the economy as well as key drivers for development in all sectors. Governments, businesses, public and private organizations, and individuals have become dependent on the digital environment for their core activities.

Therefore, they all face a growing number of uncertainties. Cyber, digital and ICT hardware and software security threats and incidents have increased, leading to significant financial, privacy and reputational consequences, and in some cases even to physical damage. Digital security incidents can have far-reaching economic consequences for organizations. Examples include disruption of operations (denial-of-service attacks, disruption of information assurance and sabotage), direct financial loss of hundreds of billions of euros, lawsuits, reputational damage, the theft of intellectual property, technology and research, loss of competitiveness (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 information being shared among partners is a key value of public-private partnerships (PPPs). 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 critical sectors, across sectors, nationally and internationally — is vital to effectively address the cyber security challenges of organizations. One of the key outputs of information sharing is the establishment of trust between people and organizations. Information sharing is an effective approach for managing collaborative cyber risk in a domain where the threat landscape is continuously changing. The sharing or exchange of information is increasingly encouraged by legislators and other stakeholders who recognize that reducing cyber security 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.

It is often said that information is power, and information being shared among partners is a key value of public-private partnerships. This concept is particularly true in a world that moves at the speed of light — internet speed.

No organization can address the full spectrum of its cyber security and cyber resilience on its own. Organizations are trending toward global interconnectedness and are consequently exposed to equally global cyber security threats. Collaboration with partners across organizational, functional, sectoral and national boundaries, and from small and medium enterprises up to multinational private enterprises and governments, is therefore required. This is essential to counter dynamic and multidisciplinary cyber security threats which may negatively impact an organization and its services. Moreover, in most cases critical infrastructure 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.

It is essential to create an atmosphere in which both public and private parties show awareness of each other's need for discretion and act accordingly.

PPPs are used by public and private sector organizations to share information about incidents, vulnerabilities, threats, related strategic topics, operational methods and best practices. A number of countries, such as Germany, the Netherlands, the United Kingdom and the United States, have gained substantial experience with PPPs where they have brought together key stakeholders, including government, national agencies, regulators, information technology (IT) companies, IT security firms, business enterprises, private critical infrastructure and security researchers. This cooperation has evolved disparately, depending on the environment, culture and legal framework of a given country. Some of these PPPs have been legislatively or regulatorily mandated. Others have been developed by like-minded organizations of their own accord.

KEYS TO SUCCESS

Creating trust is vital for the success of any PPP because information shared within a PPP is often sensitive. It is essential to create an atmosphere in which both public and private parties show awareness of each other's need for discretion and act accordingly. Building trust is especially important when an initiative is based on voluntary information sharing and membership. In a trust-reliant PPP, it should be clear to all partners that the goal of cooperation is not 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. Information sharing and analysis centers or information sharing and analysis organizations and the use of Traffic Light Protocol and of other standards establish rules on how information should be communicated. Within a framework of building trust there is significant value in 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.

Continuous interaction between stakeholders is needed to foster cooperation. Trust is also built by establishing co-leadership of programs and consensus partnership decision-making. 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 goals and establish incentives for partners. Another key to success is a clear common interest that establishes a basis for cooperation and creates a win-win situation. 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).

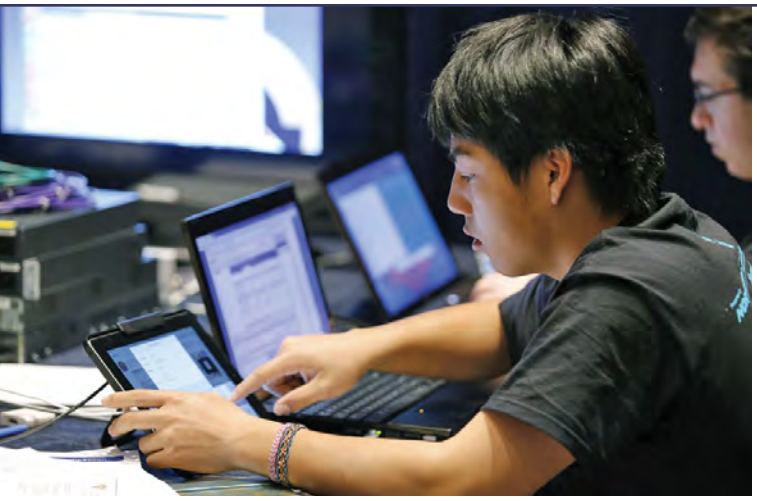
To avoid misunderstandings and mistakes, clarity about tensions and competing agendas is needed. If the partners' interests are not well-aligned,

Australian Foreign Minister Julie Bishop, center, visits the Telstra security operations center before speaking at Australia's inaugural International Cyber Engagement Strategy at the Telstra Customer Insight Centre in Sydney in October 2017.
EPA

governance by rules is advised. An awareness of each other's priorities, goals and limitations is necessary. This prevents conflict through misjudgment. Both public and private parties should know what drives each other and be able to evaluate whether 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 own mandate and standard operating procedures. Moreover, an organization's top management needs to have a clear view of the objectives and how they benefit the business objectives of that organization in areas such as the protection of shareholder interests.

Sharing of information is a significant benefit of a PPP. It is crucial that each partner provide equal value in-kind for information received within an appropriate time frame. This encourages each participant to cooperate and increases trust in the partnership. A secondary and equally important benefit is building individual personal networks. As mutual trust gradually increases, further information sharing is inspired. Energetic engagement by each participating organization helps build momentum by continuously adding value to all stakeholders. Senior-level commitment of public and private sector partners to the partnership process should be communicated to staff.

PPPs work best when the collaborating organizations operate at a similar 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 its ability to professionally and securely handle sensitive information received from other organizations. However, in some communities not all organizations are equally as capable or mature as others. Larger



The cyber defense competition CyberCenturion, a partnership of Northrop Grumman, the U.S. CyberPatriot Nation Youth Cyber Education Program and Cyber Security Challenge U.K., helps address the cyber skills gap.

THE ASSOCIATED PRESS/ GLOBE NEWSWIRE

organizations still may benefit from protecting and investing in information sharing with smaller organizations because this can positively impact a sector's image. Organizations have different backgrounds and ways of operating, especially in an international context. They have their own culture, history, language, judicial system, political and ethical differences, as well as experiences, norms, procedures, processes and practices. Some are public and some private, and some are more open to cooperating than others.

Language differences can stem not only from translation between different languages, but also from different vocabulary or 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 may help to stimulate the information flow between diverse communities. Moreover, organizations should not be pressed to share information against their wishes. If required to do so, their reluctance may be demonstrated negatively, for example, by overloading the recipient with low-value information. However, in some instances such as cases of national security and public safety, there may be a need for mandatory incident reporting. An ongoing debate rages between mandatory and voluntary information sharing. This is not an exhaustive list of key factors for the establishment or maintenance of successful PPPs, but they are characteristics worthy of consideration that have been identified by numerous research studies.

CHALLENGES

There are many challenges for PPPs 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 because of laws and regulations. Further, the high expectation that threat information shared from the public to the private sector will be accurate leads to extensive and stringent review and revision processes that delay the release of time-critical information. High public-sector staff turnover often hinders effectiveness, especially regarding trust issues. Hesitation to share information may also stem from the fact that passive and perhaps noncontributing members of PPPs are not penalized or because the conditions to join some PPPs are rather informal. A lack of respect for the confidentiality of information or for established rules of cooperation to which stakeholders have agreed could be even more counterproductive for a PPP. An efficient information exchange between organizations from different countries is also hindered by different laws and local regulations imposing data localization requirements and information storage restrictions, as well as information secrecy and nondisclosure rules.

Certain countries or sectors presume information sharing on cyber incidents may ultimately be interpreted through local or European regulations as anti-competitive behavior and, hence, likely to infringe on competition rules. Furthermore, law enforcement and other public officials may have multiple conflicting tasks and role ambiguity. Sharing detailed threat information to enhance common situational awareness may also, under certain legal frameworks, oblige a law enforcement official to change hats and use that information for investigative purposes. As a result, the source of the information may be leaked in the courts or may damage the reputation of the affected organization(s). National laws and regulations on personal data protection are additional barriers in the information-sharing process. For example, 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.** A PPP should be informed by knowledge of the partners most appropriate to accomplish its goals. Both public and private entities have vested (though varying) interests in cyber security 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 cyber security. The engagement of state, local and territorial government entities 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 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 cyber security — as are their academic counterparts in either

European Commission Vice President Andrus Ansip, from left, European Union Security Union Commissioner Julian King and EU Digital Economy and Society Commissioner Mariya Gabriel speak about cyber security in Brussels. REUTERS

arena. It is equally important that private-sector partners include industry entities of varying size, from the largest corporations to small startups. Further, while the support of senior leaders from each sector is vital, it is equally important that partnerships extend to the tactical levels within partner organizations to ensure that the most nuanced engagement occurs between experts at any rank.

Building together the cyber security ecosystem fosters national and business goals as it provides market development and public safety.

- **Establish clarity regarding tensions and competing agendas.**
  Government stakeholders appear to approach cyber security as a matter of national security. They require information and expertise from private-sector entities to secure cyberspace effectively, and thus consider partnerships a public good. In contrast, their private-sector counterparts appear to view cyber security 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 positive gains for both partners.**
  Trust is essential to all successful relationships and can be built only over time and, primarily, through personal relationships. PPPs should implement policies which maintain continuity of membership, backed by incentives. Having the right people in the partnership is another way to develop trust. Members that bring value that cannot be gained elsewhere will increase the motivation to build trusted relationships. In addition, trust must be built both ways. This means a recipient of information will not abuse it nor cause harm to the source, but must also trust in the source to 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 to give the source confidence that the information will only be used as agreed. Moreover, in some cases it is necessary to include nondisclosure agreements, and arrangements for sharing sensitive information.

- **Develop incentives on behalf of the public enterprise.**
  As much as trust-building is vital in developing true partnerships, Rachel Nyswander Thomas and Larry Clinton stress in their respective studies for the Center for Strategic and International Studies and in the *Journal of Strategic Security* that 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 through better security and resilience; cost savings from sharing the labor 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; leveraging the skills, experience and organizational positions of other members; and revoking membership for not contributing or attending meetings.

- **Establish a legal/regulatory framework.**
  The proliferation over the past decade of PPPs focused on securing cyberspace suggests that legislation is not necessary for public and private entities to work with one another. However, legislation could help create a regulatory environment more conducive to voluntary partnerships such as those in the financial or telecommunications sectors. Measures clarifying the authority various public institutions have to aid the private sector in the case of cyber intrusions would enable such public institutions to respond to requests better and in a timely manner, making private entities more likely to see value in partnership. Such 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 cyber security is a matter of national security, it

Germany's telecommunications giant Deutsche Telekom AG opened Europe's largest integrated Cyber Defense and Security Operation Center in Bonn in October 2017.
REUTERS

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 cyber security PPP. This does not preclude regulatory mechanisms to encourage accountability, 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 (U.K. 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 the PPP and 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.

THE WAY FORWARD

Public-private partnerships remain a vital and effective tool for achieving national and business cyber security goals. Common efforts to prevent, protect against, mitigate and recover from attacks are the best way to secure cyberspace. But to shift the balance in favor of resilience and strong protection, while at the same time allowing innovation, requires resources focused on research and development, technical standard setting, national and international policy development, and the building of human capital. Building together the cyber security ecosystem fosters national and business goals as it provides market development and public safety. □

The views expressed in this article 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.