ETH zürich

ETH Library

Trusting Technology: Smart Protection for Smart Cities

Other Publication

Author(s):
Baezner, Marie; Maduz, Linda; Prior, Tim

Publication date:
2018-11-07

Permanent link:
https://doi.org/10.3929/ethz-b-000300581

Rights / license:
In Copyright - Non-Commercial Use Permitted

Originally published in:
CSS Analyses in Security Policy 235

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

No. 235, November 2018, Editor: Benno Zogg

Trusting Technology: Smart Protection for Smart Cities

Smart cities need smart Critical Infrastructure Protection. This means trusting technology to play a more substantial role in securing infrastructure for the resilient provision of critical services. Adapting to a future that includes Artificial Intelligence and the Internet of Things is a necessity, not a choice.

By Marie Baezner, Linda Maduz and Tim Prior

A man stands at the main hall during the Internet Security Conference 2018 in Beijing, China, September 4, 2018. *Jason Lee / Reuters*

Connectedness within and between modern societies generally strengthens social systems. But connectedness can also increase the exposure and sensitivity of technical systems to disturbances (natural, technical, and social). When those technical systems provide critical services for social systems, connectivity can become a problem.

Modern societies would be unsustainable without certain critical services like water, electricity, food, transport, security, etc. These services are often produced, distributed, or dependent on critical infrastructure (CI). The convenience of these services makes cities attractive places to live and work. Given that CIs form the substrate on which services supporting daily life rely, securing these infrastructures is of paramount importance. Accordingly, Critical Infrastructure Protection (CIP) has become a regional, national, and multinational security priority.

Global urbanization and the increasing complexity of CI systems are accompanied by an exponential acceleration of technological development. Technological advances, like those being made in Artificial Intelligence (AI), are often touted as panaceas for a future characterized by complexity and connectivity. Are we confident enough to trust their promised benefits in the protection of critical services though? This question must be examined in light of the possibility that if the tools and processes of CIP are not adapted to the future urban reality, we may not be capable of securing the provision of critical services in the future.

The Internet of Things and CIP

The city of the future will likely be built on a cyber-physical platform characterized by interconnected critical "systems of systems" – for instance, an interdependent energy-communication-health system. The future "Smart City" will feature smart grids, which are distinguished from traditional CI grids by serving as bi-directional information communication systems linking critical service providers and consumers. Smart grids draw on various devices installed in CIs and at consumers' premises to monitor, analyze, and control the effective-

© 2018 Center for Security Studies (CSS), ETH Zurich

ness, efficiency, reliability, security, sustainability, and stability of the service.

Smart grids are made functional by the "Internet of Things" (IoT). The rapid digitalization of all aspects of modern society has been the principal driver of the rise of the IoT, which refers to the interconnections (over the internet) between computing devices embedded in household and industrial objects. In the context of smart grids and CI, the IoT provides the underlying structure by which objects and devices are connected, automated, and monitored. While the connectivity of modern devices makes many aspects of daily life more effective and convenient, the producers and users of such devices often neglect their security.

Improvements in machine learning are likely to have implications for CI and its protection.

Recent research (Huq/Hellberg 2017, see box) shows that devices connected over the IoT and utilized by critical sectors including the emergency services, financial services, utilities, and education are highly exposed to cyber-threats. Because these devices often do not support a user interface and are consequently very difficult or impossible to set up or update, many continue to operate using insecure default settings. This insecurity exposes these devices to malicious access, creating potential entry points for malicious cyber-activities that could disrupt the provision of critical services.

Three types of IoT devices can be associated with CIs: 1) devices in households like smart lighting, refrigerators, or security systems, 2) devices embedded in the CIs themselves, like metering sensors or Supervisory Control and Data Acquisition (SCADA) systems, and 3) devices embedded in industrial machinery that are not directly connected to CIs, but could be used to access CIs indirectly (e.g., SCADA systems on an automated car production line). Each type of device presents different security issues for CIs. On the level of individual households, this might create problems of data or identity theft, or allow malicious actors to access CI networks. Because these devices are also connected directly (smart meters and grids) or indirectly (routers, refrigerators, media players, printers, etc.) to local, regional, and national CI networks, the consequences of malicious penetration experienced at the household level may have cascading consequences through the IoT. This will present a significant future problem in the context of CIP, principally because the security of connected household and industrial IoT devices may never meet the same security standards as those applied to CI objects.

The ability to anticipate these developments in the context of effective CIP may depend on other important trends. In particular, technological trends (like automation and the development of AI) will expose significant legacy and modernization challenges (associated with aging CI), not just for CI operators, but also for those charged with CIP. A major task of the future CIP manager will be to ensure that cities' CI is fit for the service it is designed to provide when faced with a vast intensification of use associated with urbanization.

CIP and the Age of AI

One of the most significant technological advances that will change our future is the development of AI. While the speed at which this technology will become a part of everyday work and life continues to be debated, there is no question that the technology will have positive and negative implications for society. Indeed, discussions between those people anxious about the use and abuse of AI, and those proclaiming the technology as a multi-problem solution tool, are robust and continuous.

At this stage, AI continues to be restricted to narrow, specialist task domains, a form of AI termed Artificial Narrow Intelligence (ANI) – Google Assistant and Apple's Siri are good examples. The advance to "strong", or human-level AI has not yet been reached, despite a massive scientific push for its advancement (see CSS Analysis 220). Even so, AI development has occurred more quickly than expected, especially in the AI sub-domain of machine learning (Allen/Chan 2017, see box).

Improvements in machine learning, especially with respect to computer programming in the context of CI operations, are likely to have implications for CI and its protection. Machine learning is ultimately at the root of modern automation. Through machine learning, AI can improve programming efficiency and could even create its own code. Most importantly for security, AI could increase program functionality, especially during updates, which could be pre-tested for vulnerabilities or bugs prior to deployment. However, problematically, AI could also be used maliciously to program sophisticated malware that can rapidly adapt and may be difficult to detect and stop. In the right hands, though, machine learning is also rated as a fundamental tool in future CIP as part of intelligent Intrusion Defense Systems (Cazorla et al. 2013, see box).

Given the nature of CI as typically providing a narrow range of services, the level of AI currently available is well-suited to CIP, where it can be directed at improving the efficiency of specialized tasks. As the technology advances, more and more processes, including those tasks typically restricted to human operators, will fall into the capabilities of AI. For example, the management and oversight of currently automated control systems is likely to become a task of human-level AI in the future. Already now, the process of risk analysis, a fundamental activity in the protection of CI, is considered to be an area where AI will excel. Here, the ability of machine intelligence to weigh risks and responses objectively, using long-term operational data collected from a broad range of interconnected "smart" sensors and devices, will quickly exceed the subjective capabilities of the human risk manager.

"Smart" CIP for Smart Cities?

Switzerland's CIP is arguably more decentralized than that of many other states, reflecting the Confederation's subsidiary structure. At present, CIP is conducted in a cross-cutting strategic manner, combining the need to manage traditional natural, social, and technical hazards with cybersecurity and national economic supply. Following national guidelines for overall critical infrastructure resilience, and with the support of the cantons, the protection of CI is the responsibility of the CI operator.

Traditionally, CIP has been strongly focused on the physical security of objects like power lines, generators, roads, and hospitals. But recently, the focus has shifted to the services that CI objects help to deliver for the population, like healthcare, financial services, telecommunications, and mobility. This change reflects the fact that it is the services in our "smart" societies that make infrastructures critical, and that services are provided by a system composed of many connected CI objects. If we focus our attention on the protection of individual objects, which may be owned and managed by

© 2018 Center for Security Studies (CSS), ETH Zurich

different operators, the complete system that provides the service may be overlooked – a case of not seeing the wood for the trees. Moving from a focus on the security and protection of objects to the security and protection of services will encourage a focus on systemic CI security and protection principles. In concrete terms, this means shifting CI protection goals from the security of objects to securing the delivery of critical services.

The IoT will further enhance the decentralized nature of the management and protection of Switzerland's critical infrastructure systems. Here, AI will play an important role in permitting CI managers to corral and utilize connectivity for the purpose of securing and protecting CI. Decentralized approaches to security could present potential solutions to hyper-connected, but exposed, critical infrastructures. For example, smart grid sensors or internet-connected devices across a multi-sector infrastructure system should not only serve as conduits for information between service providers and consumers to optimize the delivery of that service. They could also be used to supply information on the security situation of that service or device and alert the operator to object or device vulnerability, cyber-attacks, or malfunctions.

IoT-connected sensors and devices could also be used to return real-time information on the state of implementation of CIP measures. Given the volume of information involved under these new circumstances, machines will increasingly shoulder the lion's share of this work. Proponents of AI, machine learning, and automation argue that CI processes supported by these technologies are likely to be significantly more efficient than current human-controlled systems.

Both risks and benefits can be found in any new technology or practice.

The potential for highly decentralized security, delivered through the IoT, could be supplemented by a distributed ledger. Distributed ledger security, most notably exemplified by the blockchain technology developed to secure the Bitcoin cryptocurrency, offers a novel approach to securing internet-connected devices in a decentralized system. Blockchain technology separates a system into individual "blocks", each of which stores security information about the system. In order to access or change the system, a command must be approved by each block before the change or access to the system is permitted.

Using the devices associated with smart grids, together with technology like AI and distributed ledgers, CIP managers can be better prepared to meet the changing circumstances of the age – especially those presented by the IoT. However, if the opportunities new technologies present cannot be grasped because we don't trust them to fulfil traditionally established tasks in securing CI, then Smart CIP will not be realized.

Trusting Technology

There is an undeniable tension between the pursuit of convenience and the increasing criticality of infrastructure. In this context, nervousness about new technology is not new, nor is it unwarranted. Complexity and connectedness arguably have negative implications for security, especially if they are neither acknowledged nor addressed. New technologies and developments like AI and the IoT, which may be synonymous with advancement, also bring uncertainties. A crucial challenge for the modern CIP manager is the need to strike a balance between the preservation of security and the openness to exploit opportunities that come with advancement and the accompanying uncertainty.

It is difficult to estimate how useful technologies like AI and blockchain will be in the future. However, the challenges that smart grids and the IoT in Smart Cities will pose for future Critical Service Protection may also bring hidden opportunities for security and protection – if we are ready to take advantage of them. Organizational advancement often happens as a process of opportunism – taking chances when they are offered. Both risks and benefits can be found in any new technology or practice. If "no risk" is the criterion determining the adoption of any new technology or practice in organizational development and adaptation, then benefits will go undiscovered.

Security organizations in particular tend to resist change. This is perhaps because change can be perceived as instability, which might affect the accomplishment of important tasks. But security can also be compromised if "practices that were once helpful become harmful under altered circumstances" (Wildavsky 2017, see box). The hyper-connectedness and complexity of modern CIs, and the appearance of AI as a game-changing technology, are altering the circumstances under which CI protection has hitherto operated.

Challenges on the Road to Smart CIP

All appropriate measures, actions, and practices must be taken to secure and protect CI "systems of systems" and the services they provide. As the circumstances of CIP change, identifying and prioritizing new measures for security and protection becomes as important as identifying new risks and threats. Technology must play a role in this context. Addressing other important future organizational, technical, and social challenges, like modernizing legacy systems and training an appropriately skilled workforce, will establish the basis on which new technologies can be trusted in future Critical Service Protection.

Under circumstances of rapidly advancing technology and the increasing complexity of cyber-physical infrastructure systems, aging infrastructure objects present a significant challenge. In the past, the standardization of parts, techniques, policies, and processes have streamlined CIP activities, but actions suitable for the recent past may constitute obstacles or have harmful

Further reading

Huq, N., Hilt, S. & Hellberg, N. **US Cities Exposed: Industries and ICS. A Shodan-Based Security Study of Exposed Systems and Infrastructure in the US.** (2017).

Wildavsky, A. **Searching for safety. Searching for Safety** (2017).

ECORYS UK. **Digital Skills for the UK Economy.** (2016).

Schuetze, J. **Warum dem Staat IT-Sicherheits-expert:innen fehlen. Eine Analyse des IT-Sicherheitsfachkräftemangels im Öffentlichen Dienst.** (2018).

Cazorla, L., Alcaraz, C. & Lopez, J. Towards automatic critical infrastructure protection through machine learning. See: **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 8328 LNCS,** 197–203 (2013).

Allen, G. & Chan, T. **Artificial Intelligence and National Security.** (2017).

© 2018 Center for Security Studies (CSS), ETH Zurich

implications in the near future. The modernization of so-called "legacy systems" through the application of new technologies to meet the reality of an IoT world will be a challenging task in the reliable provision of critical services over the next decade. For example, employing a CI object-focused approach to risk management may be suitable for examining and addressing the physical security of that object, but the process will be insufficient for examining and managing the security of a CI system and the service it provides.

It is possible that many aspects of CI and its protection will be automated in the near future.

It is possible that many (if not all) aspects of CI and its protection will be automated in the near future. Whether or not we're ready for such a future in the context of protecting critical services is an important question, but it's a *fait accompli* in the absence of a human workforce capable of operating under such circumstances. Recent research suggests that, although dedicated education initiatives exist (ECORYS UK 2016, see box), developments in cyberspace and technological advancements in the economy have already outpaced the transfer of experts from universities to positions of responsibility, deepening an already significant human-machine interoperability gap in industry (Schuetze 2018, see box). Based on the example presented in the preceding paragraph, a CI risk manager who lacks the skills to interact with a machine-based process of risk analysis, which draws on the vast quantity of data associated with a modern CI system, will find it difficult to interpret and use the resultant analysis to optimize critical service protection.

These challenges create additional uncertainty in the world of Critical Service Protection. Indeed, they further aggravate the uncertainties already associated with the arrival of technologies like automation and machine learning, and a context of infrastructure systems seamlessly connected through the IoT. These challenges must be met and addressed on the road to developing "smart" critical service protection. In this context, trusting and introducing new technologies that can support critical service protection in a suitable operating environment will be much less troublesome.

Marie Baezner is a Researcher in the Cyber Defense Group of the Center for Security Studies (CSS) at ETH Zurich, and author of "Cybersecurity in Sino-American Relations" (2018).

Linda Maduz is a Senior Researcher in the Risk & Resilience team at CSS/ETH.

Dr. Tim Prior is Team Head Risk & Resilience at CSS/ETH and author of "Measuring Critical Infrastructure Resilience" (2015), among other publications.

CSS Analyses is edited by the Center for Security Studies (CSS) at ETH Zurich. Each month, two analyses are published in German, French, and English. The CSS is a center of competence for Swiss and international security policy.

Editors: Christian Nünlist, Fabien Merz, Benno Zogg
Layout and graphics: Miriam Dahinden-Ganzoni
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000300581

Feedback and comments: analysen@sipo.gess.ethz.ch
More issues and free online subscription:
www.css.ethz.ch/en/publications/css-analyses-in-security-policy

© 2018 Center for Security Studies (CSS), ETH Zurich