Une protection intelligente pour des villes intelligentes

Les villes intelligentes ont besoin de protection intelligente pour leurs infrastructures critiques. Mais pour cela, il faut avoir confiance en la technologie et en sa capacité à jouer un rôle de plus en plus important dans la sécurisation des infrastructures afin de garantir la fiabilité et la résilience des services critiques. Évoluer vers un avenir qui inclut l'intelligence artificielle et l'Internet des objets est une nécessité et non un choix.

Par Marie Baezner, Linda Maduz et Tim Prior

Un participant se tient debout dans le hall principal lors de la «Internet Security Conference 2018» à Beijing en Chine le 4 septembre 2018. *Jason Lee / Reuters*

La connectivité, telle que nous l'observons parmi les sociétés modernes, renforce généralement les systèmes sociétaux. Toutefois, elle peut aussi augmenter la vulnérabilité et la sensibilité des systèmes techniques aux perturbations (naturelles, techniques ou sociales). Lorsque ces systèmes techniques fournissent des services critiques aux systèmes sociétaux, la connectivité peut alors devenir un problème.

Les sociétés modernes ne seraient pas durables sans l'existence de certains services critiques, comme la gestion de l'eau, de l'électricité, de l'alimentation, des transports, de la sécurité, *etc.* Or, ces services sont produits, distribués ou dépendants des infrastructures critiques (IC). La commodité de ces services fait des villes des lieux de vie et de travail attrayants. Les IC étant le substrat sur lequel reposent les services venant en soutien de la vie quotidienne, il est extrêmement important de sécuriser ces infrastructures. C'est la raison pour laquelle la protection des infrastructures critiques (PIC) est devenue une priorité, que ce soit à l'échelle régionale, nationale ou internationale.

Parallèlement à l'urbanisation mondiale et à la complexité croissante des systèmes IC, le développement technologique progresse à une vitesse vertigineuse. Les avancées technologiques telles que nous les connaissons dans le domaine de l'intelligence artificielle (IA) sont souvent vantées comme la panacée face à un avenir caractérisé par la complexité et la connectivité. Sommes-nous cependant assez confiants pour croire aux bénéfices que l'on nous promet en matière de protection des services critiques? Cette question doit être examinée à la lueur de la possibilité que, si les outils et processus de protection des infrastructures critiques ne sont pas adaptés à la future réalité urbaine, nous pourrions être incapables à l'avenir d'assurer certains services critiques de manière sécurisée.

L'Internet des objets et la PIC

La ville de demain sera vraisemblablement construite sur la base d'une plate-forme cyber-physique caractérisée par des «systèmes de systèmes» critiques interconnectés – par exemple, un système de fourniture d'énergie-communication-santé interdé-

pendant. Les «smart grids» ou réseaux (électriques) intelligents sont une composante caractéristique de la «smart city» du futur dans laquelle le réseau IC traditionnel sera remplacé par des systèmes d'information et de communication bidirectionnels reliant les fournisseurs et les consommateurs de services critiques. Les «smart grids» font appel à différents appareils installés au sein des infrastructures critiques et chez les consommateurs pour surveiller, analyser et gérer l'efficacité, l'efficience, la fiabilité, la sécurité, la durabilité et la stabilité du service.

Le fonctionnement des réseaux intelligents repose sur l'Internet des objets (Internet of Things, abrégé en IoT). La numérisation rapide de tous les aspects de la société moderne a été le principal moteur du développement de l'Internet des objets, qui réfère aux interconnexions (via Internet) existant entre les appareils informatiques présents au sein des ménages et des objets industriels. Dans le contexte des «smart grids» et des infrastructures critiques, l'Internet des objets met à disposition la structure sous-jacente nécessaire à la connectivité, à l'automatisation et au suivi des objets et appareils connectés. Mais tandis que la connectivité des appareils modernes améliore l'efficience et la commodité de bien des aspects de la vie quotidienne, les fabricants et les utilisateurs de ce genre d'appareils négligent souvent leur sécurité.

Des récentes recherches (Huq/Hellberg 2017, cf. encadré) ont montré que les appareils connectés via l'Internet des objets et utilisés par des secteurs critiques, dont les services de secours, les services financiers, les services aux collectivités (utilities) et l'éducation, étaient lourdement exposés aux cyber-menaces. Souvent, ces appareils sont dépourvus d'interface utilisateur. Il est donc très difficile, voire impossible, de changer les paramètres ou de les mettre à jour, de sorte qu'ils restent programmés sur des paramètres par défaut pas sécurisés. Cette insécurité expose ces appareils à des tentatives d'accès illicites, créant des points d'entrée potentiels pour des cyber-activités malveillantes susceptibles de perturber la fourniture de services critiques.

Trois types d'appareils basés sur l'IoT peuvent être associés aux infrastructures critiques: 1) des appareils présents au sein du foyer, comme des systèmes d'éclairage, des réfrigérateurs ou des systèmes de sécurité intelligents, 2) des appareils incorporés aux infrastructures critiques, tels que des capteurs de mesure ou des systèmes de contrôle et d'acquisition de données (SCADA) et 3) des appareils intégrés dans des installations industrielles qui ne sont pas directement connectés à des infrastructures critiques, mais qui pourraient être utilisés pour y accéder de manière indirecte (par exemple, des systèmes SCADA présents sur une chaîne de production automobile automatisée). Chaque type d'appareil présente différents problèmes de sécurité pour les infrastructures critiques. Cela peut engendrer des problèmes de vol de données ou d'identité à l'échelle des foyers, ou permettre à des acteurs malveillants d'accéder aux réseaux des infrastructures critiques. Étant donné que ces appareils sont également connectés directement (compteurs intelligents, réseaux) ou indirectement (routeurs, réfrigérateurs, lecteurs multimédias, imprimantes, etc.) aux réseaux IC locaux, régionaux et nationaux, les conséquences d'une intrusion malveillante au niveau du foyer peuvent avoir des répercussions en cascade. Cela posera à l'avenir un problème majeur dans le contexte de la protection des infrastructures critiques, d'autant que la sécurité des foyers connectés et des appareils industriels basés sur l'IoT pourrait bien ne jamais être astreinte aux mêmes standards de sécurité appliqués aux objets IC.

Anticiper ces évolutions dans l'optique d'une PIC efficace implique sans doute de devenir dépendant d'autres tendances majeures. Certaines tendances technologiques, comme l'automatisation et le développement de l'intelligence artificielle, poseront en particulier des challenges en terme de modernisation (liés au vieillissement des IC), non seulement pour les opérateurs d'infrastructures critiques, mais aussi pour les acteurs chargés de gérer la protection de ces infrastructures. L'une des principales missions du futur responsable de la PIC consistera à garantir que les infrastructures critiques des villes seront capables d'assurer les services pour lesquels elles ont été conçues lorsqu'elles seront confrontées à une utilisation massive et à une population urbaine croissante.

La protection des IC

L'une des avancées technologiques majeures appelées à bouleverser notre avenir est le développement de l'intelligence artificielle. Si la vitesse à laquelle cette technologie sera intégrée à notre vie de tous les jours continue à faire débat, il ne fait en revanche aucun doute qu'elle aura des implications positives et négatives pour la société. De fait, les discussions entre ceux qui s'inquiètent de l'usage et des abus de l'intelligence artificielle et ceux qui proclament qu'il s'agit d'une solution apte à résoudre de multiples problèmes sont aussi animées qu'incessantes.

À ce stade, l'IA demeure limitée à quelques domaines restreints et spécialisés, sous une forme appelée «artificial narrow intelligence» (ANI) ou intelligence artificielle restreinte – l'assistant Google et l'assistant virtuel Siri d'Apple en sont de bonnes illustrations. Le stade de l'IA «forte» (c'est-à-dire développée à un niveau équivalent à l'esprit humain) n'est pas encore atteint en dépit des efforts déployés par les scientifiques (cf. Analyse CSS 220). Malgré cela, le développement de l'intelligence artificielle a été plus rapide que prévu, notamment dans le sous-domaine du machine learning (Allen/Chan 2017, cf. encadré).

> Les progrès du machine learning sont susceptibles d'avoir un impact sur les IC et leur protection.

Les progrès du machine learning, tout particulièrement en ce qui concerne la programmation informatique dans le contexte du fonctionnement des infrastructures critiques, sont susceptibles d'avoir un impact sur les IC et leur protection. Le machine learning est à la base de l'automatisation moderne. Appliquée à ce domaine, l'IA est en mesure d'améliorer l'efficience de la programmation, et pourrait créer son propre code. Mais ce qui est essentiel pour la sécurité, c'est que l'IA pourrait accroître la fonctionnalité des programmes, notamment lors des mises à jour qui pourraient faire l'objet de tests préliminaires visant à détecter les failles ou les bugs avant leur déploiement. Cependant – et c'est bien là ce qui pose problème –, l'intelligence artificielle pourrait aussi être utilisée pour programmer des logiciels malveillants sophistiqués, capables de s'adapter rapidement et potentiellement difficiles à détecter et à contrer. Placé entre de bonnes mains, à l'inverse, le machine learning est considéré comme un outil déterminant pour la PIC du futur dans le contexte des systèmes intelligents de défense contre les intrusions (Cazorla et al. 2013, cf. encadré).

Au vu de la nature des infrastructures critiques, qui servent généralement à la fourniture de services restreints, le niveau d'intel-

ligence artificielle actuellement disponible convient parfaitement pour la PIC, un domaine où elle peut être exploitée pour améliorer l'efficience de tâches spécialisées. Avec les avancées technologiques, de plus en plus de processus, dont les tâches traditionnellement réservées aux opérateurs humains, tomberont sous les compétences de l'IA. Ainsi, la gestion et la supervision de systèmes de commande actuellement automatisés pourraient à l'avenir être assurées par l'IA «forte». À l'heure actuelle, on considère déjà que le processus d'analyse des risques, qui constitue une activité essentielle dans le contexte de la protection des infrastructures critiques, est un domaine dans lequel l'IA est appelée à exceller. À cet égard, l'aptitude de l'intelligence machine à peser objectivement les risques et les réponses en exploitant les données opérationnelles recueillies sur le long terme grâce à une multitude de capteurs et d'appareils «intelligents», tous interconnectés, dépassera rapidement les capacités subjectives du gestionnaire de risques humain.

PIC intelligent

La protection des infrastructures critiques en Suisse est davantage décentralisée que dans bien d'autres pays, reflétant en cela le principe de subsidiarité ainsi que la structure de la Confédération. En l'état actuel des choses, la PIC est gérée selon une stratégie transversale combinant la nécessité de gérer les risques naturels, sociaux et techniques traditionnels avec la cybersécurité et l'approvisionnement économique du pays. Conformément aux directives nationales en matière de résilience des infrastructures critiques, et avec le soutien des cantons, la protection des IC relève de la responsabilité de l'opérateur.

La protection des infrastructures critiques était traditionnellement fortement axée sur la sécurité physique d'objets tels que les lignes électriques, les générateurs, les routes et les hôpitaux. Toutefois, on observe une focalisation de plus en plus forte sur les services que les infrastructures critiques aident à dispenser à la population, comme les soins, les services financiers, les télécommunications et les services de mobilité. Cette évolution reflète le fait que ce sont les services proposés dans nos sociétés «intelligentes» qui rendent les infrastructures critiques, et que ces services sont fournis par un système composé de nombreux objets IC connectés. Si nous restons concentrés sur la protection d'objets individuels, dont la propriété et la gestion peuvent être entre les mains de différents opérateurs, nous risquons de ne pas voir tout le système qui fournit le service. En déplaçant notre attention de la sécurité et la protection d'objets vers la sécurité et la protection de services, nous encourageons une plus forte concentration sur des principes de sécurité et de protection systémiques des infrastructures critiques. Concrètement, cela signifie un glissement des objectifs de protection des IC de la sécurité des objets vers la sécurisation de services critiques.

L'Internet des objets va intensifier la décentralisation de la gestion et de la protection des systèmes d'infrastructures critiques en Suisse. L'IA est appelée à jouer là un rôle important en permettant aux gestionnaires d'infrastructures critiques d'organiser et d'exploiter la connectivité pour sécuriser et protéger les IC. Les approches sécuritaires décentralisées pourraient constituer des solutions potentielles pour les infrastructures critiques hyper-connectées, mais exposées. À titre d'exemple, les capteurs de réseaux intelligents ou les appareils connectés à Internet au sein d'un système d'infrastructure multi-secteurs ne devraient pas se contenter de fournir des informations devant circuler entre le fournisseur et le consommateur du service dans le but d'optimiser la fourniture de ce service. Ils pourraient également être utilisés pour délivrer des informations sur la situation sécuritaire du service ou de l'appareil, ou sur des problèmes de vulnérabilité, de cyberattaque ou de dysfonctionnement de l'objet ou de l'appareil.

Les capteurs et appareils connectés via Internet des objets pourraient aussi être exploités pour renseigner en temps réel sur l'application ou la non-application des mesures de protection des infrastructures critiques. Compte tenu du volume d'informations en jeu dans ces nouvelles conditions, les machines à IA devront assumer la majeure partie de ce travail. Les défenseurs de l'intelligence artificielle, du machine learning et de l'automatisation argumentent que les processus IC supportés par ces technologies sont susceptibles d'être nettement plus efficients que les systèmes courants gérés par des humains.

Le potentiel de sécurité hautement décentralisé offert grâce à l'IoT pourrait être complété par un système de registres distribués. La sécurité par registres distribués, dont l'exemple le plus célèbre est la technologie de la «blockchain» ou «chaîne de blocs» développée pour sécuriser la cryptomonnaie «Bitcoin», constitue une nouvelle approche pour sécuriser des appareils connectés à Internet au sein d'un système décentralisé. La technologie «blockchain» sépare un système en «blocs» individuels, chacun de ces blocs contenant des informations relatives à la sécurité du système. Pour accéder au système ou le modifier, la commande doit être approuvée par chaque bloc avant que l'accès ou le changement soit autorisé.

En utilisant les appareils en association avec des réseaux intelligents, ainsi qu'avec des technologies comme l'intelligence artificielle et les registres distribués, les responsables de la protection des infrastructures critiques peuvent être mieux préparés à l'évolution des conditions – et notamment aux évolutions liées à l'IoT. Toutefois, si les opportunités que présentent les nouvelles technologies ne peuvent pas être saisies parce que nous ne les croyons pas capables d'accomplir des tâches traditionnelles de sécurisation des infrastructures critiques, alors la protection intelligente des infrastructures critiques restera lettre morte.

Faire confiance à la technologie

Il existe de toute évidence un paradoxe entre poursuivre sur la voie de la commodité et augmenter la criticité des infrastructures. Dans ce contexte, l'inquiétude à l'égard des nouvelles technologies n'a rien de nouveau et est tout à fait justifiée. La complexité et le tout-connecté ont, il est vrai, des impacts négatifs sur la sécurité, a fortiori si on ne leur accorde pas la considération et l'attention requises. Les nouvelles technologies et évolutions telles que l'intelligence artificielle et l'Internet des objets,

Lecture ultérieure

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. Cf. **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).

qui peuvent être synonymes de progrès, apportent elles aussi leur lot d'incertitudes. Trouver le bon équilibre entre la préservation de la sécurité et la possibilité d'exploiter les opportunités résultant du progrès et des incertitudes qui l'accompagnent, tel est le dilemme fondamental que tout responsable PIC doit aujourd'hui tenter de résoudre.

Il est difficile d'évaluer la véritable utilité des technologies comme l'intelligence artificielle et la «blockchain» dans des circonstances futures. Toutefois, les défis que les réseaux intelligents et l'Internet des objets appliqués aux villes intelligentes poseront à l'avenir en termes de protection des services critiques pourraient bien receler également des opportunités pour la sécurité et la protection – pour peu que nous soyons disposés à en profiter. L'évolution des organisations est souvent le résultat d'un processus opportuniste, les chances étant saisies au moment où elles s'offrent. Toute nouvelle technologie ou pratique comporte des risques et des avantages. Si le critère déterminant pour l'adoption d'une telle technologie ou pratique dans le cadre du développement et de l'adaptation d'une organisation est «zéro risque», alors les avantages resteront occultés.

Toute nouvelle technologie ou pratique comporte des risques et des avantages.

Les organisations en charge de la sécurité, notamment, tendent à résister au changement. Une explication réside peut-être dans le fait que le changement peut être perçu comme un facteur d'instabilité susceptible d'impacter l'accomplissement de tâches importantes. Mais la sécurité peut aussi être compromise si «des pratiques qui étaient autrefois utiles deviennent nuisibles dans des circonstances altérées» (Wildavsky 2017, cf. encadré). L'état hyper-connecté et la complexité des infrastructures critiques modernes, de même que l'émergence de l'intelligence artificielle en tant que technologie capable de changer les règles, sont en train de modifier les conditions dans lesquelles la protection des IC s'est opérée à ce jour.

Sur la voie de la PIC intelligente

Toutes les mesures, actions et pratiques appropriées doivent être mises à profit afin de sécuriser et protéger les «systèmes de systèmes» IC et les services qu'ils fournissent. Avec l'évolution des conditions dans lesquelles s'opère la PIC, l'identification et la hiérarchisation des nouvelles mesures de sécurité et de protection deviennent tout aussi importantes que la détection des nouveaux risques et menaces. La technologie a un rôle à jouer dans ce contexte. La gestion d'autres enjeux organisationnels, techniques et sociaux futurs importants, comme la modernisation des systèmes hérités et la formation de personnel qualifié, permettra de poser les bases de nouvelles technologies de confiance pour la protection des services critiques de demain.

Dans un contexte marqué par les progrès rapides de la technologie et la complexité croissante des systèmes d'infrastructure cyber-physiques, les objets d'infrastructure vieillissants représentent un enjeu majeur. Par le passé, la standardisation des pièces, techniques, directives et processus a permis de rationaliser les activités de protection des infrastructures critiques. Par contre, certaines actions considerées comme appropriées pour un passé proche peuvent devenir des obstacles ou avoir des implications négatives à court terme. La modernisation des «systèmes antérieurs» grâce à l'application de nouvelles technologies, dans le but de rejoindre la réalité d'un monde basé sur l'IoT, sera l'un des défis à relever pour garantir la fiabilité des services critiques au cours de la prochaine décennie. Ainsi, l'adoption d'une approche de gestion des risques centrée sur l'objet IC pourrait être un moyen adéquat pour aborder et assurer la sécurité physique de cet objet, mais le processus ne suffira pas pour examiner et gérer la sécurité d'un système IC et le service qu'il fournit.

On peut imaginer qu'un grand nombre d'aspects (sinon leur totalité) touchant aux infrastructures critiques et à leur protection seront automatisés dans un avenir proche. Que nous soyons ou non préparés à un tel avenir dans le contexte de la protection des services critiques,est une importante question. Cependant on risque de se retrouver devant le fait accompli si le personnel humain opérationnel dans ces conditions est absent. De récents travaux de recherche suggèrent qu'en dépit des projets d'enseignement spécialisé qui existent (ECORYS UK 2016, cf. encadré), le transfert de l'éducation vers l'occupation de postes est distancé par les avancées technologiques en cours dans le secteur de l'économie, creusant encore le fossé déjà important de l'interopérabilité homme-machine (Schuetze 2018, cf. encadré). En se basant sur l'exemple présenté au paragraphe precédent, il résulte qu'un gestionnaire de risque IC ne possédant pas les compétences pour interagir avec un processus d'analyse des risques basé sur le machine learning qui exploite les énormes quantités de données allant de pair avec un système IC moderne, aura des difficultés à interpréter et à exploiter les analyses en résultant pour optimiser la protection des service critiques.

Ces défis génèrent des incertitudes supplémentaires dans l'univers de la protection des services critiques. Certes, ils aggravent les incertitudes déjà associées à l'arrivée de technologies telles que l'automatisation et le machine learning et exagèrent un contexte dans lequel les systèmes d'infrastructure sont parfaitement connectés via l'Internet des objets. De tels défis doivent être pris en compte et relevés sur la voie du développement de la protection «intelligente» des services critiques. Il sera alors bien moins difficile de faire confiance à de nouvelles technologies capables de contribuer à la protection des services critiques et de les mettre en œuvre dans un environnement opérationnel adéquat.

Marie Baezner est chercheuse au sein du Cyber Defense Group du Center for Security Studies (CSS) à l'EPF de Zurich, et auteure de «Cybersecurity in Sino-American Relations» (2018).

Linda Maduz est chercheuse senior au sein de l'équipe Risk & Resilience du CSS/EPF.

Dr. Tim Prior est chef de l'équipe Risk & Resilience du CSS/EPF et auteur de «Measuring Critical Infrastructure Resilience» (2015), entre autres publications.

Les analyses de politique de sécurité du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH Zurich. Deux analyses paraissent chaque mois en allemand, français et anglais. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale.

Editeurs: Christian Nünlist, Fabien Merz, Benno Zogg
Relecture: Fabien Merz
Layout et graphiques: Miriam Dahinden-Ganzoni
ISSN: 2296-0228; DOI: 10.3929/ethz-b-000300594

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Téléchargement et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

Les politiques d'armement européennes No 234
La politique de Trump au Moyen-Orient No 233
Les défis du contrôle des armements nucléaires No 232
Le Bélarus entre Est et Ouest No 231
Externalisation – le pari de l'UE sur les migrations No 230
Gestion de la religion dans les conflits: l'approche suisse No 229