

Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Souveraineté dans le cyberspace
Autor: Lutz, Heinz
DOI: <https://doi.org/10.5169/seals-823456>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

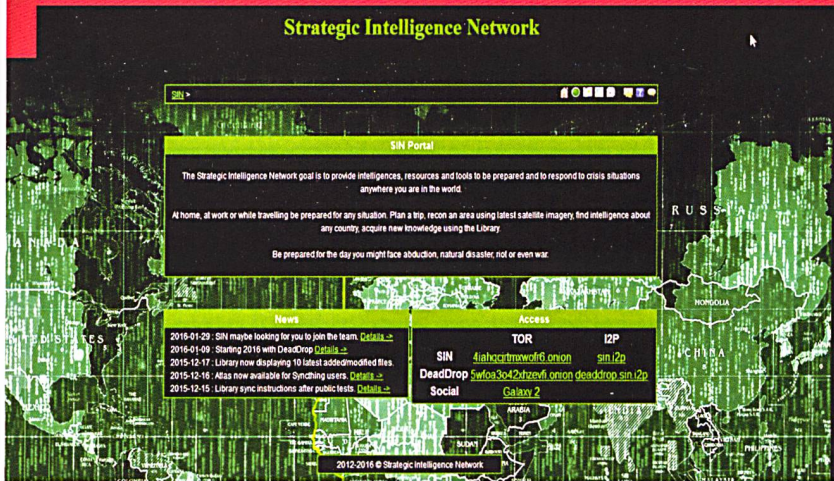
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 12.05.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>



Roschi Rhode & Schwarz est une entreprise spécialisée dans la protection des réseaux informatiques et de communication militaires. L'entreprise est basée à Ittigen dans le canton de Berne.

Cyber

Souveraineté dans le cyberspace

Heinz Lutz

Vice President, Defense & Government, Rhode & Schwarz Cybersecurity GmbH

La protection des infrastructures critiques et de leurs données est devenue un défi particulier pour les acteurs étatiques et militaires – ceux-ci sont de plus en plus confrontés à des menaces multidimensionnelles asymétriques et numériques. Dans ce contexte, ils ne doivent pas renoncer à leur souveraineté sur leurs ressources numériques critiques de l'Etat.

Le cyberspace est devenu un champ de bataille permanent où les acteurs étatiques et non étatiques s'affrontent afin d'obtenir une influence à la fois économique et politique. Mais les cybermenaces ne s'arrêtent pas aux frontières nationales. Cela exige non seulement la protection des organisations politiques, militaires et de renseignement, mais aussi le développement de stratégies actives pour leur défense – ainsi que des échanges sécurisés avec des partenaires internationaux.

Dans un monde en mutation numérique et devant faire face à des menaces asymétriques, la cybersécurité est devenue une condition préalable pour les gouvernements et leurs représentants diplomatiques, militaires et de renseignement, ainsi que pour les organisations. La protection appropriée des informations classifiées est indispensable : pendant la création, le stockage et la transmission des données. L'augmentation du nombre d'appareils en réseau entraîne simultanément une augmentation des cyber-risques.

La transformation numérique en constante évolution exige une réorganisation de notre économie et de notre société. Pour survivre en toute sécurité et compétitivité dans ce monde de plus en plus interconnecté, les gouvernements et les organisations militaires et civiles ont besoin d'infrastructures numériques fiables pour assurer et fournir leurs services aux citoyens et aux partenaires.

Pour fonctionner avec succès et protéger les ressources,

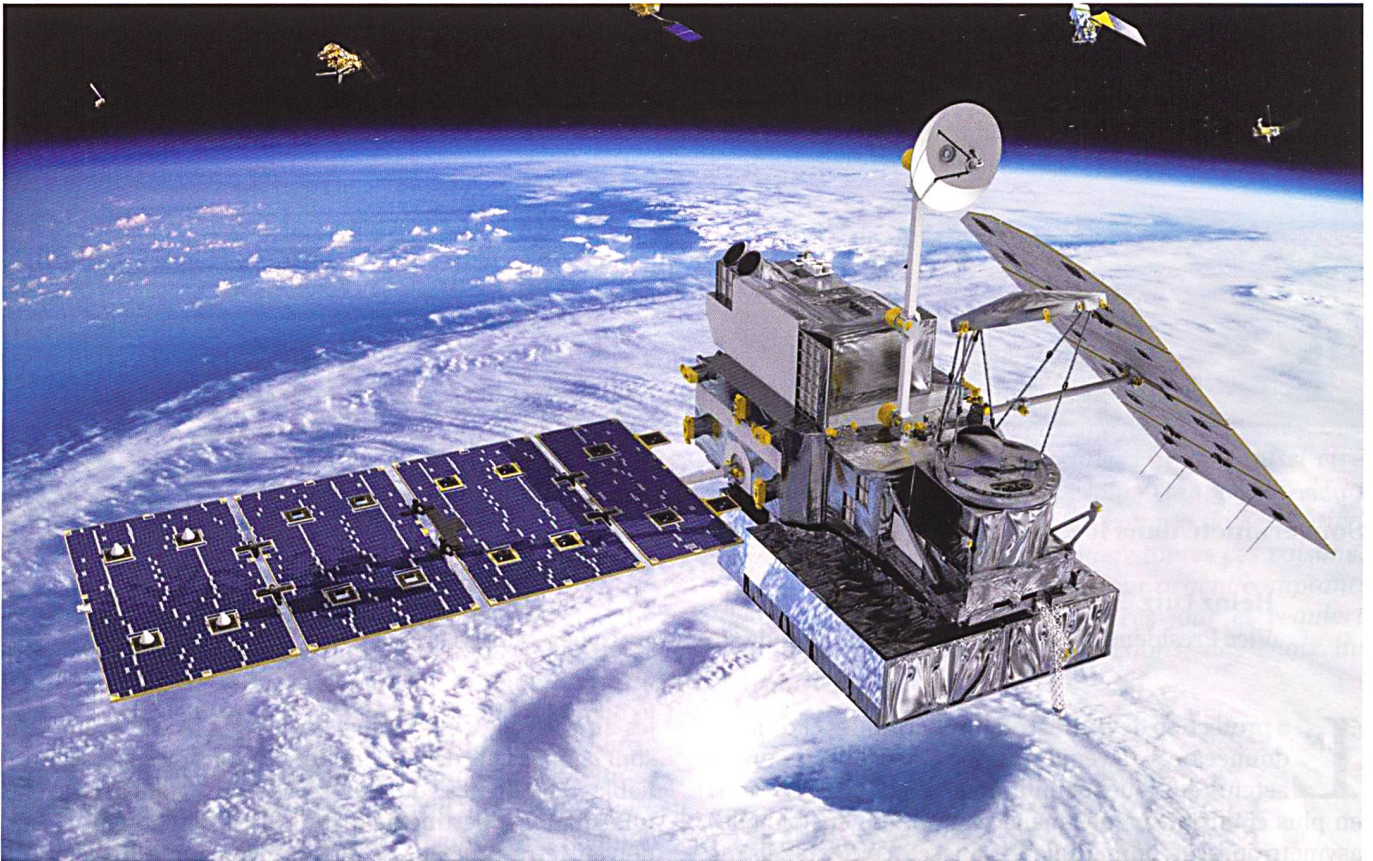
les infrastructures critiques et les personnes qui leur sont confiées, ils dépendent de solutions de cybersécurité fiables et dignes de confiance. C'est ainsi que les informations pertinentes pour la protection de l'Etat doivent être protégées contre l'accès non autorisé et la manipulation tout au long de leur cycle de vie. En même temps, ces informations doivent être disponibles pour les personnes autorisées, rapidement en toute sécurité et de n'importe où dans le monde.

Ce n'est que si l'échange sécurisé d'informations entre tous les organismes concernés est garanti que ceux-ci sont en mesure de mener à bien leurs tâches et leurs missions importantes.

La cryptographie s'est imposée comme une technologie clé pour la protection des informations numériques et jouera un rôle clé pour façonner et faire progresser l'innovation dans le domaine de la numérisation, par exemple la technologie de la chaîne de blocs. En tant que noyau du cryptage des informations sensibles, la cryptographie devra de plus en plus répondre aux exigences nationales dans le monde entier afin de garantir la souveraineté sur les infrastructures et les données numériques au sein du pays. L'agilité cryptographique d'une solution de cybersécurité joue ici un rôle essentiel.

L'agilité cryptographique des solutions garantit que les procédures de cryptage peuvent être adaptées précisément aux besoins respectifs des utilisateurs, afin de répondre aux exigences nationales pour des niveaux de classification élevés (CONFIDENTIEL et SECRET). De plus, les fonctions cryptographiques doivent soutenir pleinement le cycle de vie de la solution de cybersécurité. Un exemple à cet égard est la mise à disposition en temps voulu de procédures cryptographiques « prêtes à l'emploi. »

Les forces armées, sur terre, en mer et dans les airs, dans

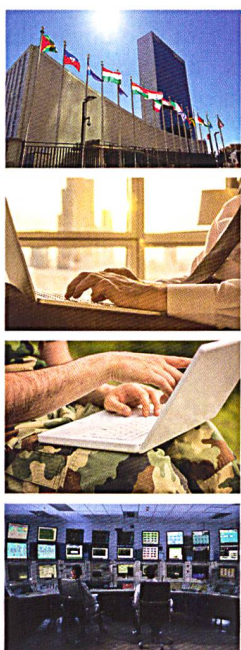


le cyberspace – ainsi que les organisations, les services de renseignement et les protections des frontières, en tant qu'acteurs centraux de la politique de sécurité nationale et internationale, ont besoin d'un partenaire technologique digne de confiance à leurs côtés qui connaît, comprend et est en mesure de satisfaire à leurs besoins spécifiques.

Grâce à de nombreuses années d'expérience dans tous les segments de la sécurité informatique, Rohde & Schwarz Cybersecurity offre une protection intelligente

avec des solutions de cybersécurité fiables, dignes de confiance, conviviales et sophistiquées. Grâce à l'agilité cryptographique de ses solutions de sécurité, Rohde & Schwarz Cybersecurity est le partenaire idéal pour la sécurité des ressources critiques. Les solutions éprouvées de cyberdéfense et de cybersécurité sont appréciées dans le monde entier par les gouvernements, les organisations militaires et les opérateurs d'infrastructures critiques.

H. L.




Enabled for
Cryptographic Agility

1. Network Encryption – on Ethernet level
2. Network Encryption – on IP level
3. Mobile Security
4. Endpoint Security
5. Cloud Security
6. Network Threat Intelligence
7. National Crypto Program and Knowledge Transfer



Parce que vos objectifs sont proches des nôtres.

ELCA Business Line „Defense & Cybersecurity“

- Offre des solutions IT de qualité suisse, neutres, du conseil jusqu'à l'opération des systèmes
- Large expertise métier dans les domaines de la défense et des forces de l'ordre, mise en œuvre dans des systèmes au cœur du métier sécuritaire
- Compétence reconnue dans le domaine de la cybersécurité en aidant les agences gouvernementales et les compagnies privées à sécuriser leur environnements IT
- Offre un conseil spécialisé en servant d'intégrateur de proximité et en développant des solutions sur mesure
- Neutre, pas de dépendances vis-à-vis des éditeurs
- Fournisseur de logiciel depuis 30 ans pour l'armée suisse et les forces de sécurité civile
- Habilité à travailler sur les systèmes et domaines classifiés les plus critiques
- Capacité à gérer des projets sur site client tout comme en hébergeant les systèmes dans nos infrastructures sécurisées

Proposant une gamme complète de solutions métier et technologiques, ELCA est l'un des plus grands prestataires indépendants de Suisse et une entreprise leader dans les domaines du conseil en informatique, du développement et de la maintenance de logiciels ainsi que de l'intégration de systèmes informatiques. Les solutions d'ELCA réduisent la complexité et accélèrent les cycles d'innovation, augmentent les résultats commerciaux et la satisfaction des clients. La société privée, qui compte plus de 920 experts, possède des succursales à Lausanne, à Zurich, à Genève, à Berne, à Paris, à Madrid, à Bâle, à Grenade et à Hô Chi Minh-Ville (développement délocalisé) qui opèrent toutes selon des processus communs.

www.elca.ch

**ELCA**
We make it work.