Guerre de l'information

Cybersécurité: Défis pour la Suisse politique

Etat des lieux

La guerre de l'information est une menace croissante, notamment pour les démocraties occidentales dont tous les acteurs sociaux sont touchés. Dans ce chapitre, nous identifions en particulier la nécessité d'intervenir auprès des acteurs étatiques, afin d'identifier leur rôle et leurs tâches et de mettre en lumière les champs d'action prioritaires.

La thématique de la guerre de l'information («Information Warfare» en anglais) a une longue tradition, au niveau international comme en Suisse. À la fin des années 1990 et jusqu'en 2010 environ, le terme générique couvrait tous les sujets pertinents, de la guerre dans le cyberespace à la propagande, en passant par la désinformation ou encore la guerre psychologique. Le sujet a été traité à la fois dans le cadre de l'Exercice de conduite stratégique 97 (ECS) et conceptuellement au sein de l'armée suisse dans le cadre de l'étude conceptuelle *Information Operations* (KS IO). Aujourd'hui, l'utilisation de ce terme se réfère principalement à la manipulation de l'opinion publique à l'aide de méthodes sémantiques, les aspects technologiques constituant l'un des moteurs d'exécution de ces opérations.

Dans les années 1990, diverses organisations et chercheurs ont attiré l'attention sur les développements possibles de l'utilisation de la technologie numérique pour la production et la diffusion répétées d'informations manipulées. Cependant, ce n'est qu'avec l'avènement des réseaux sociaux et la disponibilité à large échelle des technologies d'apprentissage automatique/en profondeur à des prix abordables que cette problématique est devenue pertinente et concrète.

L'utilisation d'algorithmes d'intelligence artificielle, l'automatisation et la présence d'immenses quantités de données sur internet et les réseaux sociaux modifient l'ampleur, la portée et la précision d'utilisation des campagnes de propagande informatisées pour manipuler l'opinion publique.

Recommandations

1. Augmentation des aptitudes de l'État à agir au niveau de la détection et de l'attribution des opérations d'influence. Implication de tous les niveaux de l'État (fédéral, cantonal, municipal) et coordination sur le plan fédéral.
2. Révision des bases juridiques pour permettre de riposter aux opérations d'influence et établissement de directives claires concernant les options de défense ou les contre-attaques possibles.
3. Travail avec les médias nationaux pour détecter la désinformation et sensibiliser le grand public à la problématique.
4. Conclusion d'accords avec d'importantes plateformes sociales, qui peuvent être utilisés en Suisse comme support pour lutter contre les opérations d'influence des réseaux sociaux.
5. Création d'un système d'alerte pour les attaques en cours (à l'instar de SwissAlert ou similaire).
6. Coordination politique avec l'Union européenne pour lutter contre les opérations d'influence des réseaux sociaux, p. ex. en interaction avec les plateformes de réseaux sociaux.
7. Assimilation des connaissances des réseaux sociaux et sensibilisation aux risques numériques dans les programmes éducatifs.
8. Soutien aux initiatives de fact-checking spécifiquement axées sur le contexte suisse.

Aujourd'hui, il est possible de produire du contenu automatiquement ou semi-automatiquement, de le convertir en textes, en paroles et en images et de le rendre accessible à une masse ciblée de personnes, très rapidement et sans dépenses importantes. La nature des réseaux sociaux les rend particulièrement vulnérables aux attaques. Il est possible de créer et d'amplifier des bulles de filtres et des chambres d'écho; des mèmes, des photos et des vidéos peuvent être utilisés pour diffuser des informations sans vérification possible de la source; des communautés peuvent être attaquées en identifiant des profils personnels vulnérables ou des nœuds influents d'un réseau.

Les réseaux sociaux sont manipulés par les gouvernements et les partis politiques. Selon une étude de l'Oxford Internet Institute[1], il existe des preuves de campagnes de manipulation des réseaux sociaux organisées par des cybertroupes ou des partis politiques dans 70 pays en 2019, contre 48 pays en 2018 et 28 pays en 2017. Les États autoritaires utilisent la manipulation des réseaux sociaux comme un instrument de contrôle de leur propre population. Les États démocratiques sont la cible d'opérations d'influence menées par une poignée d'acteurs, dont (preuves à l'appui) la Chine, l'Inde, l'Iran, le Pakistan, la Russie, l'Arabie Saoudite et le Venezuela. Aujourd'hui, la Chine compterait entre 300 000 et 2 millions de personnes au sein de ses cybertroupes. De plus, ces dernières collaborent souvent avec le secteur privé, des organisations de la société civile, des sous-cultures internet, des groupes de jeunes, des collectifs de pirates informatiques, des mouvements marginaux, des influenceurs des réseaux sociaux et des bénévoles engagés idéologiquement pour une cause.

Les techniques utilisées pour mener des opérations d'influence sont multiples, à savoir la désinformation, le piratage social, les identités frauduleuses, les robots ou encore le trolling. Toutes ces techniques ont en commun d'influencer les processus politiques (p. ex. les élections) ou même de déclencher des révoltes et des révolutions. Le potentiel déstabilisateur de ce type de guerre repose sur une compréhension plus approfondie des processus de décision humains et de la dynamique des phénomènes de masse. Ces aspects peuvent à leur tour être simulés de plus en plus facilement grâce aux nouvelles technologies et aux nouveaux algorithmes.

Défis

Changer l'opinion publique d'un pays en faveur de l'agresseur. Les démocraties où le processus de décision politique est fortement ancré dans l'opinion publique sont donc particulièrement vulnérables à ce type d'attaque.

Pour l'agresseur, les opérations de manipulation sont intéressantes à plusieurs titres:

1. elles sont relativement peu coûteuses à mettre en œuvre
2. elles sont difficiles à attribuer et le risque d'escalade est limité
3. elles permettent l'instrumentalisation à grande échelle des utilisateurs
4. elles peuvent être utilisées seules ou en combinaison avec d'autres formes de guerre (traditionnelle, économique).

D'autre part, il est difficile d'évaluer l'efficacité et l'impact des opérations d'influence. En plus, le risque existe que l'agresseur en perde le contrôle. Néanmoins, on peut considérer que ces opérations ont modifié l'opinion publique à l'occasion de plusieurs événements récents, comme les élections aux États-Unis, au Royaume-Uni et en France. La question de savoir si ces actions ont finalement été décisives reste ouverte.

Impossible également de savoir si la Suisse a déjà été la cible d'opérations d'influence élaborées. Certains éléments indiquent que de telles opérations auraient eu lieu en lien avec des thématiques politiques spécifiques (p. ex. le vote sur Billag ou la polémique sur la 5G).

1

Nécessité d'agir

La Suisse officielle estime que l'utilisation active d'informations manipulées pour atteindre des objectifs politiques n'est pas un moyen adéquat pour un État démocratique. Il est donc d'autant plus important de mettre en œuvre les actions suivantes en réponse à la menace de guerre de l'information (voir également le plan d'action de l'UE):

1. **Capacités de détection, d'analyse et d'attribution des opérations d'influence:** les actions menées par des tiers dans leur propre secteur d'intérêt doivent être **identifiées**, **analysées** et **attribuées** à un stade précoce. Il est indispensable pour cela d'avoir accès à des données pertinentes, à des outils d'analyse de données et à des capacités d'analyse humaine. Les **autorités gouvernementales** devraient être habilitées à prendre ces mesures, en collaboration avec les acteurs privés et dans le cadre d'une coopération internationale. L'analyse permanente des approches sémantiques et technologiques utilisées contribue à mettre en place et à garantir une alerte précoce. La temporalité ne doit pas être négligée: de fausses informations peuvent circuler longtemps sans être détectées et par exemple provoquer soudainement des actions violentes de la part de nombreuses personnes.
2. **Riposte aux opérations d'influence détectées**: une fois les opérations d'influences détectées, les autorités gouvernementales réagissent en se fondant sur la **base juridique** disponible. Des systèmes d'alerte, une communication basée sur les faits dans les médias ou encore la limitation des capacités de l'agresseur sont nécessaires pour réagir efficacement. Il s'agit également de permettre à sa propre population d'accéder à des informations et des faits fiables. Ce processus doit rester transparent et compréhensible afin que les informations diffusées puissent être vérifiées de manière indépendante.
3. **Collaboration entre les autorités gouvernementales et le secteur privé**: les acteurs étatiques s'appuient sur la collaboration avec le secteur privé, en particulier avec les plateformes de réseaux sociaux et les médias afin de détecter ou de réagir à la manipulation sociale. Dans des cas particulièrement graves, la collaboration peut porter sur l'accès aux données pertinentes, la fermeture de comptes suspects, la suppression de fausses informations ou l'information du grand public sur ces attaques et la correction de la désinformation.
4. **Augmentation de la résilience sociale**: comme la manipulation sociale s'adresse au grand public, il est essentiel de sensibiliser la société à ces phénomènes. Informer les personnes de tous âges sur la manière de reconnaître et de répondre à de telles attaques et impliquer la population dans des activités défensives telles que la vérification des faits font partie des mesures concrètes à mettre en œuvre.

En général, les droits fondamentaux tels que la liberté d'expression sont essentiels et fortement ancrés dans notre société – les restrictions d'accès à l'information ne sont donc justifiées qu'en dernier recours dans les cas particulièrement graves de nature pénale. Une réponse rapide sous forme d'information est donc d'autant plus importante.

Références

– Action Plan against Disinformation, Joint Communication to The European Parliament, The European Council, The Council, The European Economic and Social Committee And The Committee of The Regions, Brussels, 5.12.2018 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019JC0012

– Cyber Influence Operations: An Overview and Comparative Analysis, Center for Security Studies (CSS), ETH Zürich, Zürich, October 2019 - https://css.ethz.ch/en/services/digital-library/publications/publication.html/c4ec0cea-62d0-4d1d-aed2-5f6103d89f93

The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation. Working Paper Oxford, 2.2019 - https://comprop.oii.ox.ac.uk/research/cybertroops2019/

Annexe

Explication des formes de guerre de l'information les plus courantes

– **Désinformation**: diffusion d'informations fausses ou incomplètes dans l'intention de tromper.

– **Ingénierie sociale**: utilisation des caractéristiques sociocognitives de l'esprit humain, en particulier le tribalisme et la propension à la conformité.

– **Identités frauduleuses**: utilisation d'identités légitimes par des acteurs illégitimes.

– **Robots**: logiciels informatiques automatisés destinés à la manipulation de plateformes en ligne.

– **Trolls**: utilisateurs ou robots qui attaquent, insultent ou agressent les utilisateurs de manière ciblée.

Contact
Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
+41 44 226 50 13

https://www.satw.ch/cybersecurity-defis

Impressum
Académie suisse des sciences techniques SATW
Contributions d'experts
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Rédaction et graphisme
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
Septembre 2020