La cybersécurité: entre autonomie et soutien étatique

Présentation et analyse d'une enquête sur la position d'experts sur l'implication des différentes parties prenantes en cybersécurité sous le prisme de la transformation du Centre national pour la cybersécurité (NCSC) en office fédéral.

Melanie Knieps
Chercheuse à la Digital Society Initiative de l'Université de Zurich (UZH) et codirectrice du Cyber Resilience Network for the Canton of Zurich (CYRENZH)

Pauline Meyer
Doctorante FNS et assistante diplômée à l'Université de Lausanne

Sylvain Métille
Professeur associé à l'Université de Lausanne, avocat et docteur en droit

Markus Christen
Directeur général de la Digital Society Initiative de l'Université de Zurich (UZH) et directeur du «laboratoire d'éthique numérique» de l'Institut d'éthique biomédicale et d'histoire de la médecine de l'UZH

1. Introduction

Les développements législatifs et politiques pour réglementer le monde numérique et améliorer la sécurité des infrastructures critiques sont nombreux en Suisse comme à l'étranger. Il faut trouver le bon équilibre pour réglementer la capacité des organisations à réagir aux cybermenaces, sans pour autant la restreindre. En outre, il est important de trouver la juste balance entre l'autonomie des organisations pour se protéger et le soutien que peut fournir l'État pour augmenter leur résilience.

2. Les développements en cours

La Cyberstratégie nationale suisse (CSN) 2023 a été publiée en début d'année. Elle fait suite à la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022[1] et illustre bien les progrès de la Suisse dans le domaine. Parallèlement, la loi fédérale sur la protection des données (LPD) entrera en vigueur le 1er septembre 2023 dans sa version entièrement révisée[2] et la loi fédérale sur la sécurité de l'information (LSI) va suivre. Dans sa première version, dont l'entrée en vigueur est attendue pour début 2024, la LSI vise à garantir la sécurité des moyens informatiques et du traitement de l'information de la Confédération. Elle impose des exigences minimales en matière de sécurité de l'information pour certaines infrastructures critiques[3] et donne une base légale au NCSC, l'autorité principale en matière de cybersécurité. Le Parlement fédéral est en train de finaliser une révision de la LSI pour y ajouter une obligation de signaler les cyberattaques contre les infrastructures critiques les plus importantes sur le plan national et pour renforcer les compétences du NCSC[4].

Dans ce contexte, le Conseil fédéral a décidé de transformer le NCSC en office pour la cybersécurité[5], mais surtout de le transférer au Département fédéral de la défense, de la protection de la population et des sports (DDPS)[6]. Cette décision de transférer le NCSC au département en charge des affaires militaires et du renseignement suscite de nombreuses inquiétudes. Jusqu'à présent,

la cybersécurité était restée indépendante de la poursuite pénale et de la cyberdéfense, ce qui avait permis au NCSC de gagner la confiance des partenaires privés et des responsables de la cybersécurité des infrastructures critiques.

L'approche collaborative helvétique autour de la cybersécurité suppose une compréhension des besoins et des souhaits des différentes parties prenantes. Dans le cadre du projet de recherche NRP-77 «Promouvoir la confiance dans la cybersécurité par l'éthique et le droit» financé par le Fonds national suisse[7], nous avons interrogé 107 experts en cybersécurité, dont une majorité a pris position sur l'implication de l'État et d'autres parties prenantes.

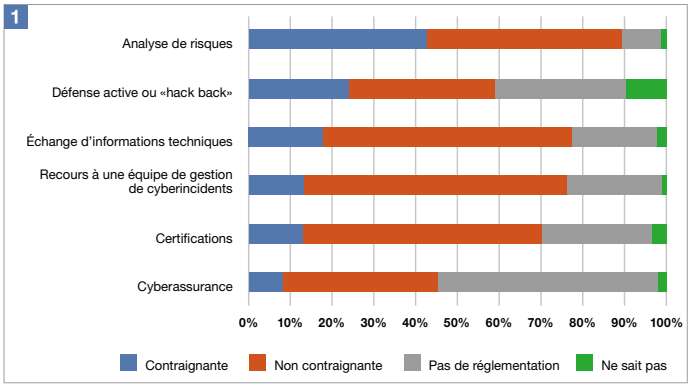
3. Réglementer principalement les mesures préventives

Les personnes actives dans le domaine de la cybersécurité doivent mettre en place des mesures préventives (pour éviter qu'un cyberincident[8] ne se produise) et réactives. Dans l'étude susmentionnée, les participants ont indiqué s'ils préféraient une réglementation obligatoire (loi ou ordonnance), une réglementation non obligatoire (lignes directrices) ou pas de réglementation (et chaque organisation peut décider elle-même de la manière de traiter le problème) pour un certain nombre de mesures. L'enquête a été menée avant et après l'annonce de transformer le NCSC, ce qui nous a permis d'évaluer l'effet de cette décision sur les opinions des participants.

Les résultats ont révélé une forte préférence pour une réglementation obligatoire pour les mesures préventives, en particulier en ce qui concerne l'analyse des risques *(cf. tableau 1)*. En revanche, lorsqu'il s'agit de mesures réactives, telles que le recours à des équipes de gestion de cyberincidents, une réglementation souple est préférée. C'est aussi le cas pour les aspects liés à la préparation individuelle, tels que la certification et l'échange d'informations techniques. Les personnes interrogées se sont finalement prononcées en faveur d'une absence de réglementation dans des domaines sans rapport avec la préparation, tels que le remboursement par une assurance du dommage lié à un cyberincident. En résumé, si les participants penchent pour une réglementation contraignante en matière de prévention des cyberincidents, ils sont en revanche favorables à une plus grande souplesse en matière de réaction aux cyberincidents.

1 Préférence pour le type de réglementation

À noter que la préférence pour la réglementation est restée élevée même après la décision de transfert du NCSC.



4. L'implication des parties prenantes

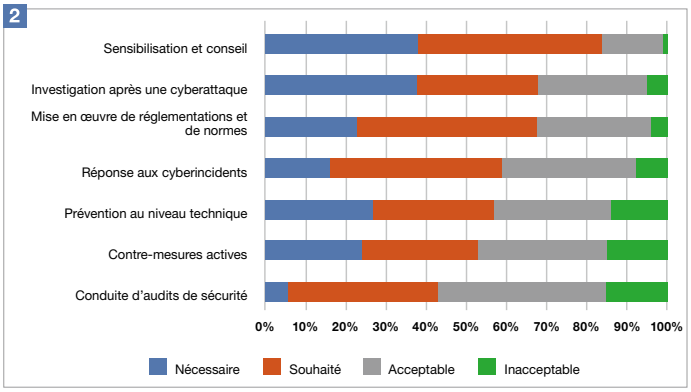
4.1 Un compromis entre autonomie et compétences

L'implication de l'État est largement acceptée lorsqu'elle sert à renforcer l'autonomie d'une organisation plutôt qu'à l'affaiblir *(cf. tableau 2)*. Le niveau le plus élevé d'acceptation de l'implication de l'État a justement été observé pour la sensibilisation et le conseil, ainsi que dans les domaines traditionnellement associés à la compétence exclusive de l'État, comme l'adoption et la mise en œuvre de réglementations et de normes ou l'investigation après une cyberattaque. L'implication de l'État semble acceptable seulement dans une moindre mesure quant au renforcement des compétences telles que la conduite d'audits de sécurité et la réponse aux cyberincidents. En d'autres termes, plus les mesures protègent l'autonomie des organisations contre les intrusions, plus l'intervention de l'État est acceptée. D'ailleurs, les organisations qui ne disposent pas d'une équipe de gestion de cyberincidents sont bien plus favorables à l'implication de l'État dans la réponse aux cyberincidents que celles qui disposent d'une telle équipe.

Dans le même ordre d'idées, l'acceptation de l'implication de l'État dans la gestion d'incidents a augmenté après la décision de transfert du NCSC *(cf. tableau 2)*[9]. L'élévation au rang d'office fédéral a mis en évidence le rôle croissant que jouera le NCSC, et le rattachement au DDPS peut laisser penser à une augmentation des capacités de défense. En résumé, l'implication de l'État est jugée acceptable tant qu'elle contribue à renforcer (sans limiter) les compétences d'une organisation contre les cyberincident

2 Préférence quant à l'implication de l'État pour la cybersécurité

La préférence pour l'implication de l'État dans la gestion d'incidents varie en fonction des capacités organisationnelles des participants et de la décision du transfert du NCSC. Alors que la plupart des participants trouvaient «souhaitable» l'implication de l'État dans la gestion de cyberincidents, ils étaient significativement plus nombreux à la juger «nécessaire» après la décision sur le NCSC. Les participants sans équipe de gestion de cyberincidents accueillent généralement mieux l'implication de l'État.



4.2 Prudence face à l'ingérence

Les mesures non intrusives, comme les campagnes de sensibilisation, sont bien acceptées. L'acceptation varie ensuite pour la prévention au niveau technique ou les contre-mesures actives. Des différences sectorielles peuvent en partie expliquer ces écarts. Le secteur des télécommunications accepte par exemple nettement moins des règles impératives concernant les mesures techniques préventives que l'administration. Cet écart peut notamment s'expliquer parce que les mesures techniques préventives sont perçues comme plus intrusives dans le secteur des télécommunications. Le bon équilibre entre le souhait d'autonomie et la plus-value de l'intervention de l'État dépend donc fortement du secteur concerné.

4.3 Pour des partenariats public-privé

Les participants à l'étude se sont généralement prononcés en faveur de l'implication d'acteurs privés et publics *(cf. tableau 3)*. En ce qui concerne les compétences fondées sur le partage de connaissances (comme la sensibilisation ou le conseil), les organisations disposant de réseaux étendus (à l'instar du NCSC, de centres cantonaux ou d'entités privées comme les centres d'analyse et de partage d'information[10]) sont préférées. Il en va de même pour la gestion de cyberincidents ou la réalisation d'audits de sécurité (bien que dans une moindre mesure pour les centres d'analyse et de partage d'information).

Des entités publiques et privées au niveau national sont privilégiées pour la prévention technique des cyberincidents: les participants ont exprimé une préférence pour la participation du NCSC, mais aussi des registres internet *(registry)*. Pour les contre-mesures actives, l'Armée suisse est intéressante aux yeux des participants. Bien que les personnes interrogées souhaitent que des partenariats public-privé (PPP) disposent de certaines compétences traditionnellement publiques, un rôle particulièrement central a été attribué au NCSC en ce qui concerne les normes de réglementation et de conformité.

En tant que principale entité compétente pour la cybersécurité en Suisse, il est tout à fait naturel que sa participation soit jugée nécessaire. Il y a une tendance similaire pour les investigations suite à des cyberattaques. Cela démontre bien une préférence pour une conservation de compétences par les autorités comme la police cantonale et les centres (cantonaux ou national) de cybersécurité. Dans l'ensemble, ces résultats montrent qu'il existe un souhait d'impliquer les entités compétentes et proches les unes des autres, que leur statut soit public ou privé.

Cela étant, la décision de transfert du NCSC pourrait avoir des conséquences inattendues sur le rôle de certains acteurs. Le souhait des participants que les registres internet assument le rôle d'enquêteurs, au détriment de la police, a augmenté de manière significative. Ce glissement des acteurs publics vers certains acteurs privés pour des enquêtes renforce encore l'idée que les experts en cybersécurité préfèrent que les autorités s'abstiennent d'interférer dans leurs affaires, en particulier lorsqu'il pourrait y avoir des inquiétudes quant à leur fiabilité. Le souhait de recourir aux PPP peut donc également être compris comme un moyen de rendre les organisations plus résilientes face aux menaces tant externes qu'internes.

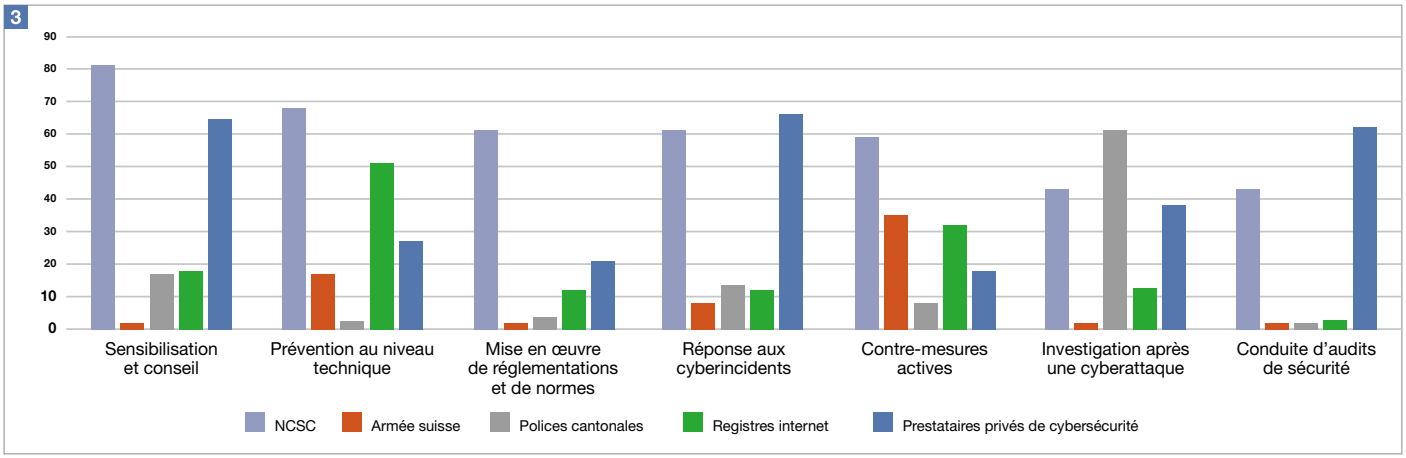
4.4 Sans surveillance excessive du NCSC

Le rôle du NCSC en tant qu'acteur étatique spécifique a été jugé acceptable (voire souhaité et nécessaire) dans la plupart des domaines, à l'exception d'un aspect particulier: des mesures qui permettraient au NCSC d'avoir un aperçu de l'activité au sein des réseaux des personnes interrogées, par exemple par le biais de capteurs exploités par le NCSC sur un réseau pour surveiller des activités malveillantes, ont été particulièrement peu acceptées.

L'acceptation de cette mesure ayant chuté de manière significative après la décision de transformation du NCSC et son transfert au sein du DDPS, on peut en déduire une baisse de la confiance. En d'autres termes, si la participation du NCSC est bien acceptée, les mesures plus intrusives sont davantage rejetées,

3 Préférences pour les implications entre acteurs publics et privés

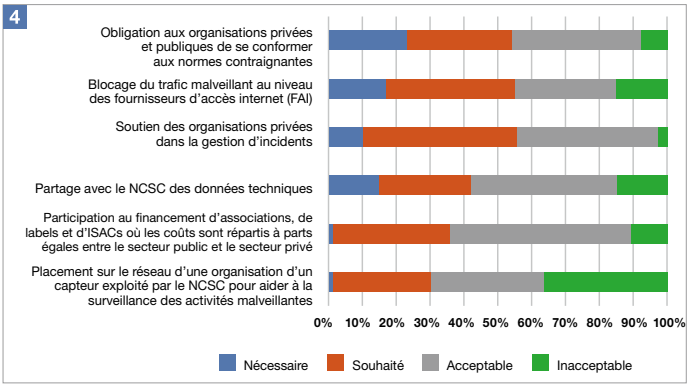
La préférence pour l'implication de la police cantonale dans les investigations a chuté de 37 (84%) avant la décision de transfert du NCSC à 24 (57%) après. La préférence pour l'implication des registres internet dans les investigations est passée de 3 (7%) avant la décision à 13 (24%) après.



en particulier lorsque l'intégrité du NCSC est questionnée, en lien avec le DDPS.

4 Préférence pour l'implication du NCSC

La préférence quant à l'implication du NCSC pour placer et exploiter un capteur sur le réseau des organisations pour aider à surveiller les activités malveillantes a chuté de manière statistiquement significative après la décision relative à son transfert.



5. Conclusion

En Suisse, la cybersécurité est un exercice délicat d'équilibre entre la préservation de l'autonomie des organisations et la nécessité de renoncer à une partie de cette autonomie pour renforcer les compétences de lutte contre les cybermenaces. Ce paradoxe entre l'autonomie et les compétences[11] est également bien visible dans le souhait de réglementation, en particulier en ce qui concerne les mesures préventives qui renforcent les compétences d'une organisation, tout en permettant une gestion souple des cyberincidents (expression de son autonomie). L'adoption d'une approche multipartite par des PPP illustre aussi l'évolution de la dynamique du pouvoir entre les entités publiques et privées. Par conséquent, cette enquête étaye l'idée selon laquelle le cyberespace remet en question les conceptions traditionnelles des principes clés de la gouvernance[12].

Les résultats de notre étude mettent également en lumière la nature complexe de la confiance, qui est généralement considérée comme une combinaison d'intégrité, de bienveillance et de compétence[13]. Par exemple, des décisions controversées telles que celle relative à la transformation et au transfert du NCSC peuvent entraîner un déplacement de la confiance, délaissant les organisations publiques comme la police pour des acteurs privés comme les registres internet.

L'acceptation de l'implication de l'État augmente et décline simultanément après la décision d'intégrer le NCSC au DDPS, ce qui souligne encore la complexité de la confiance placée en lui. En effet, l'acceptation de l'implication de la police dans les investigations et du NCSC dans le placement et l'exploitation d'un capteur sur le réseau des participants a baissé, alors qu'en parallèle le souhait pour une implication de l'État dans la gestion d'incidents a augmenté. En d'autres termes, la confiance dans les compétences de protection du NCSC augmente (dès lors qu'il profitera du niveau élevé de compétences du DDPS) mais, en même temps, la méfiance liée à son transfert au sein du DDPS augmente aussi lorsqu'il en va de compétences plus intrusives.

Au fil du temps, le NCSC et la Confédération ont grandement bénéficié de la confiance qui leur a été accordée, également en raison du développement de très nombreuses relations personnelles entre les membres du NCSC et les accords privés et publics de la cybersécurité. Il faudra particulièrement veiller à ce que le nouveau statut du NCSC permette de conserver ces personnes essentielles et à ce que la confiance dans le statut particulier du NCSC (qui lui a permis de fonctionner jusqu'ici) ne soit pas trop atteinte par sa transformation en un office, qui plus est rattaché au DDPS.

Cette contribution voulait modestement montrer quelques souhaits et besoins des experts en cybersécurité travaillant dans des infrastructures critiques et souligner l'importance de tirer parti de la confiance établie de manière encore plus efficace à l'avenir. Reste à décider de la forme que prendront les différentes interventions (publiques ou privées) et l'impact du nouveau statut du NCSC afin de concilier les intérêts des différentes parties prenantes, notamment en ce qui concerne l'autonomie et l'indépendance des organisations ainsi que leurs besoins en matière de compétences.

1 Conseil fédéral, Cyberstratégie nationale (CSN), avril 2023; Conseil fédéral, Stratégie nationale pour la protection de la Suisse contre les cyberrisques 2018-2022, avril 2018.

2 RO 2022 491; elle entrera en vigueur fin 2023.

3 RO 2022 232; art. 6 ss. LSI.

4 La version révisée de la LSI devrait entrer en vigueur en 2025. Pour plus d'informations au sujet de la LSI, voir Meyer, Métille, *Loi fédérale sur la sécurité de l'information: version 2.0*, Jusletter du 5 septembre 2022.

5 ncsc.admin.ch/ncsc/fr/home/dokumentation/medienmitteilungen/newslist.msg-id-88878.html, consulté le 19.6.2023.

6 ncsc.admin.ch/ncsc/fr/home/dokumentation/medienmitteilungen/newslist.msg-id-92048.html, consulté le 19.6.2023. Un nouveau secrétariat d'État pour la sécurité civile sera également créé au DDPS: admin.ch/gov/fr/accueil/documentation/communiques.msg-id-94386.html, consulté le 19.6.2023.

7 nfp77.ch/en/JTLSBgi4qITuxdwd/project/promoting-trust-in-cybersecurity-through-ethics-and-law, consulté le 19.6.2023.

8 Un cyberincident est «un événement survenant lors de l'utilisation de moyens informatiques et ayant pour conséquence une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations ou à la traçabilité de leur traitement», art. 5 lit. d du projet de la LSI modifiée.

9 Ce qui peut surprendre vu certaines critiques quant au rattachement militaire.

10 ISACs ou Information Sharing and Analysis Centers.

11 Bjørn Olav Knutsen, 2017. *Going Deep! Acquiring new submarines in common? An analysis of Dutch and Norwegian security interests, defence traditions and concepts for the use of submarines*, Studia diplomatica, 68(4), pp. 51-78.

12 Andrew Liaropoulos, 2016. *Exploring the complexity of cyberspace governance: state sovereignty, multi-stakeholderism, and power politics*, Journal of Information Warfare, 15(4), pp. 14-26.

13 Stephan Grimmelikhuijsen, Gregory Porumbescu, Boram Hong et Tobin Im, 2013. *The effect of transparency on trust in government: A cross-national comparative experiment*, Public Administration Review, 73(4), pp. 575-586.