# RMS+

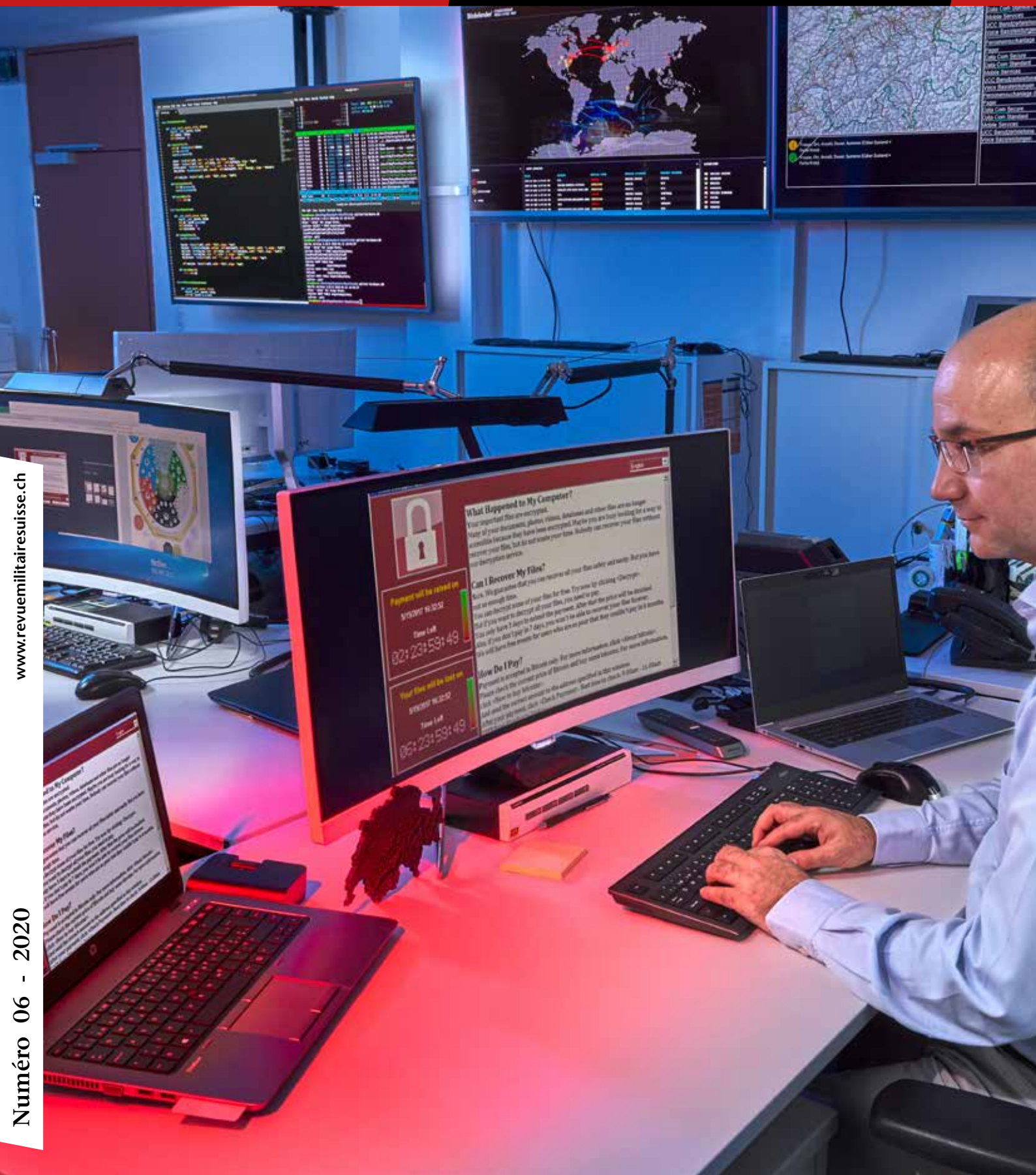
Revue Militaire Suisse

**RENSEIGEMENT**

**ARMASUISSE S+T**

**CYBER DEFENSE**

**ECONOMIE DE DEFENSE**




www.revuemilitairesuisse.ch

Numéro 06 - 2020

Revue militaire suisse N° 06 - 2020

**Il est prévu d'augmenter ces prochaines années l'effectif du personnel dans le domaine de la cyberdéfense avec la mise sur pied, le 1er janvier 2022, d'un cyberbataillon et d'un état-major spécialisé correspondant, faisant ainsi passer l'effectif actuel du personnel de milice, qui est de 206, à 575 militaires. Photo © DDPS / Jonas Kambli CC BY-NC-ND 3.0 CH.**



Ce numéro a été coordonné par le Cap Alain Mermoud.
Avec les remerciements de la RMS+

## Impressum


**Rédacteur en chef:**
Col EMG Alexandre Vautravers a.vautravers@yahoo.com

**Rédacteurs adjoints:**
Lt-col EMG Julien Grand
Cap Grégoire Chambaz
Cap Alain Mermoud

**Membres du comité:**

| | | |
|---|---|---|
| Président | Br Mathias Tüscher | mathias.tuescher@vtg.admin.ch |
| Vice-président | Col Christian Rey | info@reygroup.ch |
| Administrateur | M. Hubert Varrin | info@revuemilitairesuisse.ch |
| SMG | Maj EMG Guillaume Genoud | g.genoud@smg-ge.ch |
| SSO | Col Gianni Bernasconi | Gianni.bernasconi@bluewin.ch |
| SVO | Col Stéphane Goy | stephane.goy@multitel.ch |
| SNO | Col EMG Ivan Keller | Ivan.Keller@ne.ch |
| SOVR | Lt col Roger Haupt | roger.haupt76@bluewin.ch |
| SFO | Maj EMG Patrick Noger | patrick.noger@sfo-fog.ch |
| SJO | Col Fabien Kohler | kohler.fabien@bluewin.ch |
| SCBO | Lt-col Francesco M. Rappa | francesco@rappa.ch |

**Administration, abonnements et publicité:**
Association de la Revue militaire suisse (ARMS)
Avenue Général-Guisan 117, 1009 Pully

Tél. +41 21 729 46 44
Fax +41 21 729 46 88

Mise en pages: J-design, 1724 Bonnefontaine, jean-daniel.sauterel@bluewin.ch

Impression et distribution: Presses Centrales Lausanne S.A.

ISSN 0035-368X


La Revue militaire suisse (RMS) est un organe de publication officiel de la Société suisse des officiers. Elle appartient aux sections cantonales de Suisse romande et de Berne. Elle est éditée par l'Association de la Revue militaire suisse (ARMS).
Le but de la RMS est, notamment, de faciliter l'échange sur les problèmes militaires et de développer les connaissances et la culture générale des officiers. Les textes publiés expriment la seule opinion de leurs auteurs. La RMS est ouverte à toutes les personnes soucieuses d'œuvrer de façon constructive au bien de la défense générale.

Br Mathias Tüscher
Président de l'ARMS

Le Col EMG Haroun est le fondateur et directeur de la Pharmacie des Bergières à Lausanne.

*Editorial*

# Pour un renouvellement du principe de précaution

**Col EMG Michaël Haroun**
Stab Op S, EM instruction opérative (Formation supérieure des cadres de l'Armée)

Ecrire l'éditorial d'une RMS de si longue tradition est un privilège. Jamais pourtant son auteur n'aurait imaginé devoir attendre le résultat d'un scrutin pour oser se lancer. Et vers où ? Pour en tirer quelle conclusion ? Car dire que le 27 septembre 2020 laissera des traces profondes est un doux euphémisme.

Les années 30 où la Gauche avait finalement compris l'inéluctable dérive du monde vers la guerre et la nécessité de s'y préparer ne nous ont à l'évidence rien appris. Après avoir été surprise lors de la guerre franco-allemande de 1870, puis par la Première guerre mondiale, la Suisse s'est à nouveau trouvée dans un état grave d'impréparation au seuil d'une nouvelle conflagration qui a tué des dizaines de millions de personnes et laissé l'Europe (pour ne parler que d'elle) exsangue. Et nous remettons le couvert ?

Le très maigre résultat positif atteint dans le cadre de l'impérative modernisation de notre aviation aiguise en effet à nouveau l'appétit de ceux qui rêvent d'une Suisse sans défense. Cela n'augure rien de bon, notamment en vue du renouvellement des équipements lourds arrivant aussi en bout de vie. Une situation de blocage nous guette vraisemblablement. Avec quelles conséquences ?

Où sont nos principes d'anticipation et d'assurance « au cas où » ? La pression du quotidien, du « just in time », du « moi » à la place du « nous », du « tout de suite » à la portée de n'importe qui via son smartphone semblent avoir gommé de notre société tout bon sens. Ce constat est d'autant plus incompréhensible que le COVID vient de démontrer combien ce principe est essentiel. Cela commence, comme le disait le chef de l'Armée en 2014, très critiqué à tort, par « … avoir quelques réserves à la maison ». Mais une part importante de la population semble désormais penser que « ça n'arrive qu'aux autres ».

Après le premier accroc majeur à l'ordre international depuis la fin de la guerre froide qu'a été l'annexion de la Crimée par la Russie en 2014, les tensions se succèdent à un rythme croissant. L'affaiblissement du multilatéralisme est inquiétant. Les alliés au sein de l'OTAN – une alliance que les opposants du 27 septembre ont décrit comme notre bouclier, alors qu'ils ne manquent pas une occasion pour dénoncer son insoutenable impérialisme – en viennent même à se menacer militairement sur fond de course aux ressources énergétiques en Méditerranée. Les frictions entre la Chine et les USA, atteignent de dangereux sommets, ces derniers faisant avec leur allié japonais des exercices et simulations définissant clairement la Chine comme « l'ennemie ». D'ailleurs, que dire de cette Chine qui déclare contraire aux principes de son parti communiste omnipotent toute référence aux valeurs universelles, à la liberté de la presse et à l'indépendance de la justice qui nous sont si chères ? Et que dire aussi des USA, pilier de l'OTAN, autrefois guide de l'Occident et devenus illisibles, parfois même infréquentables ? Les rapports du Conseil fédéral et du Service de renseignement de la Confédération, pourtant on ne peut plus clairs quant au retour des tensions et des politiques de puissance, n'éveillent-ils aucune réflexion ? Si les Suédois semblent l'avoir compris, eux qui en 2018 remettaient à l'ordre du jour leur doctrine de « défense totale », la Suisse vient pourtant de montrer que sa volonté de défense se lézarde. Au seuil d'une nouvelle explosion mondiale ?

Avec Armée XXI, la Suisse caressait l'espoir d'un système de « montée en puissance ». Abandonnée depuis, cette illusion semble toujours présente dans certains esprits qui imaginent possible de se préparer au dernier moment. Aujourd'hui toutefois, l'Europe de l'industrie de la défense serait incapable de faire face aux besoins découlant d'une dégradation significative de la situation, tant en raison de ses maigres capacités, que des dominances technologiques et financières qui la minent, menaçant ainsi directement l'autonomie des nations et leur souveraineté. Quelles conséquences pour nous ? Investir fortement contre les cyberrisques est à l'évidence indispensable et en cours au DDPS, mais supposer que cela suffirait à assurer la défense de la Suisse est au mieux naïf.

Pour l'auteur de ces lignes seule vaut une vision holistique et systémique et l'ensemble des moyens y relatifs. Qui peut en effet dire avant la crise quel instruments seront indispensables ? Certes, les avions de combat n'ont pas été d'une grande utilité contre le COVID, mais *quid* des autres situations ? Leur probabilité peut apparaître encore faible, mais quand on voit la vitesse insensée à laquelle la situation évolue, on doit se préparer. Personne n'a pas le pouvoir de divination, encore moins à des horizons de 10 ou 20 ans ! Et malheureusement c'est pour le pire aussi qu'il s'agit d'être prêts à temps. Seule une boîte à outils complète permet de répondre aux menaces par nature volatiles, incertaines, complexes et ambigües. Avec le scrutin du 27 septembre, la Suisse montre qu'une majorité pourrait émerger qui serait prête à risquer de baisser les bras.

Qu'est-ce qui ne va pas chez nous ? A l'évidence, les explications de nos autorités, factuelles, honnêtes et mille fois vérifiées avant publication, font de moins en moins le poids face aux approximations, mensonges et raccourcis simplistes disponibles sans limites dans un espace informationnel toujours plus conflictuel. Il est pourtant vital que notre démocratie soit en mesure de s'exprimer en connaissance de cause sur les questions de politique de sécurité. L'émotion, les dogmes, les calculs politiques et la désinformation ne doivent pas y avoir la moindre place. On connaît certes le prix de la sécurité, mais voulons-nous apprendre dans la douleur celui de l'insécurité ? Non, alors il est urgent de redonner du sens à la sécurité – condition élémentaire de notre prospérité – et par là de redonner au principe de précaution la place centrale qui est la sienne.

M. H.

News

## Le DDPS améliore les processus d'acquisition d'armement

Berne, 15.06.2020 - L'année dernière, la conseillère fédérale Viola Amherd a demandé l'établissement d'une analyse externe dans le but d'améliorer les processus d'acquisition d'armement. Les résultats et les recommandations formulés par l'entreprise Deloitte SA et un groupe d'accompagnement sont désormais disponibles. Le DDPS les mettra progressivement en œuvre, améliorant ainsi encore les processus d'acquisition d'armement. Le rôle du Parlement quant à l'orientation stratégique à donner à l'armée s'en trouvera renforcé.

La conseillère fédérale Viola Amherd, cheffe du DDPS, s'est donnée pour but d'améliorer les processus d'acquisition d'armement. Après avoir lancé une première analyse interne l'année dernière, elle a demandé, en automne 2019, l'établissement d'une analyse externe. Il s'agissait de vérifier si et comment les processus d'acquisition pouvaient être améliorés. Il existe un risque, en particulier pour le matériel d'armement à fort contenu informatique, que les systèmes soient déjà obsolescents au moment de leur introduction auprès de la troupe.

**Une analyse externe largement étayée**

L'analyse externe a d'une part été confiée à l'entreprise Deloitte SA, qui est l'une des sociétés de gestion et de conseil stratégique les plus efficaces au monde et qui, à l'échelon international, a valeur d'experte en matière d'acquisition d'armement. Deloitte SA a présenté un rapport comprenant trois recommandations principales et cinq autres recommandations.

D'autre part, un groupe d'accompagnement composé de représentants externes a examiné les conclusions de Deloitte SA et a également formulé des recommandations. Ses membres étaient les suivants : l'ancien conseiller national Adrian Amstutz, l'ancien commandant de corps Dominique Andrey, Armin Berchtold (CEO du groupe Securitas et vice-président de la Commission de l'armement), l'ancienne conseillère nationale Corina Eichenberger, Fritz Gantert (président de la Société suisse Technique et Armée), Lukas Hupfer (directeur du Think Tank foraus) et le professeur Andreas Wenger (directeur du CSS EPFZ).

**Mise en œuvre lancée pas à pas**

Les résultats et les recommandations de Deloitte SA et du groupe d'accompagnement montrent que les processus actuels fonctionnent bien dans l'ensemble, aussi en comparaison internationale. Mais il ressort également de l'analyse que l'efficacité des processus actuels pourrait être améliorée pour ce qui est du temps, de la qualité et des coûts.

La cheffe du DDPS a maintenant demandé de mettre en œuvre ces recommandations dans les mois qui suivent.
Renforcement du rôle stratégique du Parlement

Une des recommandations principales de Deloitte SA, à laquelle le groupe d'accompagnement adhère entièrement, vise à renforcer le rôle du Parlement quant à l'orientation stratégique à donner à l'armée. Le modèle actuel prévoit que dans son message sur l'armée, le Conseil fédéral demande chaque année au Parlement des crédits d'engagement en vue d'acquérir des biens d'équipement militaires. Au lieu de cela, le Conseil fédéral devra associer plus étroitement le Parlement à un niveau plus élevé. Concrètement, le Parlement devra se pencher une fois par législature sur la question de la manière dont l'armée doit remplir son mandat à moyen et à long terme, en considération du plafond des dépenses et pour une période de quatre ans. La haute surveillance demeure garantie, car le Parlement pourra continuer à intervenir au niveau des acquisitions dans le cadre du budget annuel incluant une planification des tâches et des engagements financiers.

Ce changement renforce le rôle du Parlement dans le pilotage stratégique de l'orientation de l'armée à moyen et à long terme. En outre, une telle approche renforce la flexibilité et l'agilité des projets d'acquisition.

Un tel tournant ne peut être mis en œuvre que pas à pas et en étroite concertation avec les commissions parlementaires compétentes. Un premier échange a déjà eu lieu avec les Commission de la politique de sécurité. En fonction des résultats des entretiens qui suivront, le Conseil fédéral pourrait, en vue de la législation 2023-2027, présenter pour la première fois un message relatif à l'orientation de l'armée.

**Meilleure vue d'ensemble des projets**

Les deux autres recommandations principales émises par Deloitte SA seront mises en œuvre à l'interne du DDPS. Elles visent à mieux gérer les projets d'acquisition, actuellement coordonnés par le Groupement Défense et armasuisse. Il est de plus nécessaire d'avoir une meilleure vue d'ensemble des projets en cours, qui sont souvent interdépendants.

En outre, les unités organisationnelles qui utiliseront le bien ou le système en question seront davantage impliquées après l'approbation des projets. Le fait qu'elles devront assumer une plus grande responsabilité permet de garantir que les projets seront mis en œuvre, sur le plan du contenu, des délais et des aspects financiers, conformément à ce qui a été prévu. Les projets pourront ainsi atteindre les objectifs visés.aérien militaire. Des bases légales vont donc être créées pour une autorité du trafic aérien militaire. Celle-ci doit assurer la sécurité des Forces aériennes lors de leurs missions dans l'espace qu'elles partagent avec l'aviation civile. Elle veillera notamment à éviter tout incident ou accident dans cet espace et à garantir mieux encore la surveillance et la régulation du trafic aérien militaire. Une adaptation de la loi sur l'aviation s'impose donc.
Appui renforcé aux événements civils

Dans la foulée de la révision de la LAAM, le Conseil fédéral entend aussi renforcer l'appui apporté par l'armée aux événements civils. Cela commencera par un accroissement de la souplesse et des disponibilités de l'armée dans le sens où les recrues en phase d'instruction de base pourront, elles aussi, être engagées, et plus seulement les militaires en service long et ceux en cours de répétition. L'armée devra également pouvoir fournir des prestations dans un cadre limité lors d'événements d'importance nationale ou internationale, même sans en retirer un avantage majeur au niveau de son instruction ou de son entraînement. En introduisant cette disposition d'exception, le Conseil fédéral tient compte du fait que les événements considérés ne pourraient pas avoir lieu sans l'appui de l'armée.

De surcroît, il est aussi nécessaire que le législateur intervienne dans certains autres domaines de l'instruction – celle des militaires en service long entre autres –, dans diverses dispositions sur l'engagement

# SAMP/T

Long-Range Surface-To-Air System
For Swiss airspace protection

## Mobility

Fast deployment

Standard Modules compatible with road and infrastructure constraints

## Interoperability

NATO integrated and easy to integrate on Swiss air defense

Operates in a dense civilian airspace

## Mission-proven

Protection of sensitive areas

Operational deployments

## Simplicity

Suitable for militias

Reduced manpower

## 360° Protection

Rotating radar 1 turn/ second

eurosam
THALES MBDA

Le siège du Service de renseignement de la Confédération (SRC) à la Papiermühlestrasse 20 à Berne Berne

*Renseignement*

**Compétences du SRC en matière d'attribution des cyberattaques**

**Communication SRC**

Comme stipulé par la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), adoptée par le Conseil fédéral en 2018, il appartient au Service de renseignement de la Confédération (SRC) d'« *établir l'origine des cyberattaques (attribution) aussi précisément que possible, afin de préserver la marge de manœuvre des autorités politiques et des autorités de poursuite pénale* ». L'accomplissement de cette mission nécessite des compétences très pointues, aussi bien au niveau technique que géopolitique. Le SRC, qui intègre dans ses équipes à la fois des analystes techniques et politiques, est à même de mener à bien ce processus complexe. La tâche de l'attribution nécessite de pouvoir recourir à un large spectre de sources d'informations exclusives, qui sont à disposition du SRC.

En 2019, le SRC a enregistré une hausse sans précédent des cyberattaques d'origine étatique à l'encontre d'intérêts suisses. Alors que de nombreux États déploient des capacités d'espionnage offensives à l'étranger, y compris en Suisse, le SRC se concentre sur les services de renseignement les plus actifs et les plus agressifs contre les intérêts suisses. Dans ce contexte, le processus d'attribution des cyberattaques s'avère primordial, afin de déterminer quels Etats sont à l'origine de cyberattaques sophistiquées, principalement menées à des fins d'espionnage et souvent désignées par l'acronyme APT (« Advanced Persistent Threats »). Ces attaques sont conduites directement par des agences de renseignement ou par des groupes guidés et financés par des agences de renseignement.

Dans sa compréhension la plus basique, l'attribution consiste à identifier l'auteur d'un acte et à lui en imputer la responsabilité, autrement dit à répondre à la question « *Who did it* ? ». Concrètement, la réponse à cette question peut résulter de différents niveaux d'analyse. La forme la moins précise d'attribution consiste à désigner un type d'attaquant. On dira par exemple d'une attaque qu'elle est le fait d'un groupe criminel ou d'activistes. A un niveau de précision plus élevé, on cherchera à attribuer une attaque à un groupe d'attaquants (« *Threat actor* »). Un degré d'analyse encore plus pointu permettra de désigner un État comme responsable d'une attaque ou d'une série d'attaques. Parfois même, il sera possible de pointer du doigt une structure organisationnelle spécifique de l'Etat en question, voire des collaborateurs d'une unité spécifique à cet Etat.

**Outils à disposition des organes de sécurité suisses**

Il est dans la nature humaine de chercher, face à une agression ou à une attaque, à en identifier l'auteur, par curiosité mais également pour comprendre les raisons de cette action. Le processus d'attribution permet de mieux comprendre les motivations des auteurs et leurs modes opératoires, afin de pouvoir se protéger d'attaques ultérieures, de comprendre les stratégies géopolitiques des autres pays et d'engager des mesures de rétorsion.

En Suisse, les organes de sécurité disposent d'une marge de manœuvre pouvant se traduire en fonction du contexte par quatre types de mesures en guise de riposte à une cyberattaque:

- **Mesures basées sur la loi fédérale sur le renseignement :** il s'agit ici de mesures de recherches soumises ou non à autorisation, dirigées contre les entités ayant été identifiées, ou de mesures visant à perturber des systèmes informatiques basés à l'étranger utilisés pour attaquer des infrastructures critiques en Suisse.
- **Mesures judiciaires :** le travail d'attribution, lorsqu'il permet d'identifier précisément des entités ou

personnes, peut conduire à l'ouverture d'une procédure pénale. Le Ministère public de la Confédération (MPC) peut par exemple, sur la base d'un rapport officiel du SRC, décider d'ouvrir une enquête qui sera confiée à la police judiciaire fédérale, en particulier dans des cas d'espionnage politique ou économique.

- **Mesures administratives:** toute une série de mesures peuvent être prises contre des individus (principalement des diplomates) ayant été identifiés comme participant à des activités d'espionnage. Il s'agira par exemple d'interdictions d'entrée, de refus de visa ou d'accréditations.
- **Mesures politiques:** un dernier type de mesures est de nature purement politique. Il s'agit par exemple de thématiser la question des cyberattaques ou d'un incident spécifique lors d'une rencontre entre chefs d'Etats ou de convoquer directement un ambassadeur dans ce but. Il peut également être décidé de rendre publique une attribution, c'est-à-dire de désigner par une annonce officielle (par exemple une conférence de presse) un acteur étatique ou un pays comme responsable d'un incident, en fournissant éventuellement les détails techniques et le mode opératoire d'une attaque.

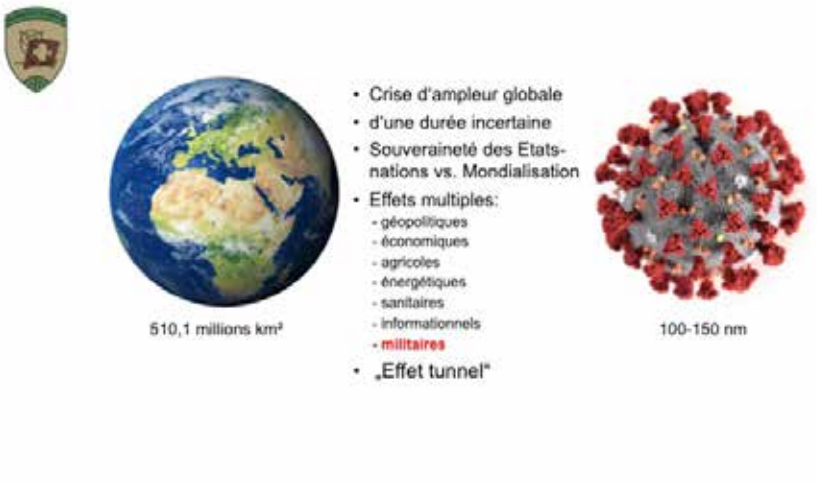
### Comment procéder à une attribution

Les méthodes permettant de procéder à l'attribution d'une cyberattaque ont donné lieu à une abondante littérature. S'il n'existe pas à ce jour une unité de doctrine absolue en la matière, les experts s'accordent tout de même sur un certain nombre de points. En premier lieu, l'attribution permet de déterminer un processus, durant lequel différentes compétences et spécialités vont intervenir. Il s'agit tout d'abord d'acquérir des informations, en particulier auprès des victimes, de services partenaires ou encore d'entreprises privées, dont des fournisseurs de service. La majeure partie de ces informations est de nature technique: échantillons de codes malveillants, informations sur l'infrastructure utilisée par l'attaquant (notamment des serveurs de commande et de contrôle), trafic, etc. L'analyse de ces données nécessite des compétences techniques pointues. Il s'agit en particulier de pouvoir relier des indicateurs entre eux et de les associer à des attaques ou à des campagnes déjà connues.

Le travail d'attribution ne se limite toutefois pas à ces aspects techniques. De nombreuses informations utiles peuvent être de nature géopolitique ou concernent les motivations de l'attaquant. Les « Advanced Persistent Threats » (APT) sont en effet alignées de manière significative sur les intérêts stratégiques des pays qui les initient, c'est pourquoi il s'agira souvent de partir des victimes pour en déduire les motivations d'un acteur précis, en considérant le contexte géopolitique (conflits, intérêts stratégiques, politique économique, etc.). Pour ce travail, c'est un autre type de compétence qui sera mobilisée, avec des analyses géopolitiques.

SRC

Le SRC exerce des compétences clés en matière d'attribution des cyberattaques.




L'appellation Service de renseignement de l'armée (SRA) englobe toutes les fractions de l'état-major et les troupes de l'armée qui assument des tâches liées au renseignement. Le Renseignement militaire (RM) représente le noyau professionnel du SRA à l'échelon du commandement de l'armée et constitue une partie du SRA.

*Renseignement*

**Tour d'horizon 2020**

**Service de renseignement militaire (SRM)**

Si une pandémie à l'échelle mondiale comme celle que nous sommes en train de vivre avait été envisagée par tous les scénarios depuis vingt ans, une crise d'une ampleur aussi grande ne faisait pas partie des hypothèses privilégiées.

Comme d'autres fléaux (la Peste noire au Moyen Age par exemple), le coronavirus a circulé le long des « routes de la Soie », qu'elles soient aériennes ou terrestres. En quelques semaines, l'hémisphère nord a été touché et les régions avec les populations les plus âgées ont été durement affectées. Du fait de son caractère brutal et massif, cette pandémie a donc constitué une véritable surprise stratégique au même titre que la chute du mur de Berlin (1989) ou la crise financière de 2008. Autre facteur déterminant, le « brouillard de l'information » qui a entouré ce nouveau virus très infectieux. Dans une société aussi informée que la nôtre, il a été frappant de constater l'ignorance dans laquelle nous nous trouvions au printemps 2020 sur un adversaire invisible, parfois assimilé au départ à une simple grippe.

A l'heure actuelle et alors qu'aucun vaccin efficace n'est encore disponible, il reste bien aléatoire de tirer un bilan exhaustif. Toutefois, certaines tendances semblent se dessiner : recul de la mondialisation au profit de la souveraineté des Nations et des frontières, retour en force de l'Etat et avènement potentiel de sociétés placées sous surveillance, manifestation de la politique de puissance sous forme d'actions politiques ou militaires opportunistes.

## Quelle mondialisation ?

Si l'on reprend les trois futurs possibles pour le monde d'ici 2035 imaginés en 2017 par la communauté américaine du renseignement (*Global Trends : The Paradox of Progress*[1]), celui des « Archipels » (un monde fragmenté) semble plus probable que ceux des « Orbites » (compétition de puissances) ou des « Communautés » (prééminence de la coopération dans un monde hyperconnecté). Il n'est pas anodin que le scénario « Archipels » prenne notamment en compte la « grande pandémie de 2023 ».

Toutefois, pas plus que la Peste noire du Moyen Age n'avait mis fin aux échanges commerciaux, la crise du coronavirus ne mettra un terme à la mondialisation. Car une société interconnectée offre en définitive plus d'avantages que d'inconvénients. En revanche, les conditions de cette mondialisation risquent de conduire à de fortes tensions internationales. A court terme (mois), les grandes en-treprises occidentales chercheront à reconstituer leurs marges et continueront donc à s'approvisionner en Asie. A moyen terme (années) toutefois, les chaînes de valeur risquent de se raccourcir, et la production *just in time* décliner. La notion de stocks stratégiques sera appliquée à la santé (aujourd'hui, 80 % des principes actifs des médicaments sont fabriqués en Inde et en Chine) mais sera certainement élargie à d'autres secteurs jugés clé (industrie aéronautique, …). La capacité d'encaisser des chocs internationaux sera un maître mot, ainsi que le retour à une certaine souveraineté étatique. A Washington comme à Pékin, les partisans du « découplage » des économies des deux pays se trouvent renforcés dans leurs positions. De manière ironique, le slogan des partisans du Brexit, « reprendre le contrôle » (« Let's take back control »), pourrait connaître de beaux jours au sein même de l'Union européenne, notamment avec la redécouverte des frontières et donc une remise en cause du principe de la libre circulation.

## Retour en force des Etats

Comme dans toute crise sécuritaire – conflit armé, terrorisme, pandémie –, les Etats se voient leur rôle renforcé, y compris dans les démocraties les plus libérales.

1 National Intelligence Council : https://www.dni.gov/index.php/global-trends-home (lien actuel)

Déploiement des forces de l'ordre le 2 juin 2020 devant le Lincoln Mémorial à Washington.

A court et moyen terme (1-2 ans), tous les gouvernements, qu'ils soient autoritaires ou non, chercheront à assurer la sécurité de leurs populations, y compris par des mesures susceptibles de remettre en cause certaines libertés individuelles. Comme le succès actuel des produits proposés par les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) le montre bien, un accroissement du rôle de l'Etat dans l'économie ne signifie pas la défaite des grands acteurs privés, en premier lieu ceux du numérique qui ont tiré profit du confinement et de la généralisation du télétravail, de la télémédecine ou de la télé-éducation. Il est probable que, comme à la suite des attentats du 11 septembre 2001, les populations acceptent dans leur majorité des atteintes significatives à leurs libertés. Et dans l'éventualité d'une résurgence du djihadisme, une sorte d'« état d'urgence permanent » pourrait s'installer et s'inspirer du cas israélien.

## Politique de puissance et risques de dérapage

Tous les Etats ont dû faire appel à leurs forces de sécurité et en particulier **à** leurs forces armées pour faire face à une situation d'urgence. Partout, les militaires ont dû se protéger contre le virus et continuer à s'entraîner pour, le cas échéant, démontrer à n'importe quel adversaire leurs capacités. Au plus fort de la pandémie, cela s'est traduit par une augmentation du nombre d'exercices et de démonstrations de force.

Certains acteurs ont ainsi profité de la concentration de la Communauté internationale sur la pandémie et de la réduction de la capacité d'intervention des grands Etats pour avancer leurs pions, que ce soit en Méditerranée orientale, en Libye ou encore en mer de Chine méridionale. Fin avril 2020 et en pleine pandémie, les dernières données sur les dépenses militaires mondiales ont été publiées[2]. Leur total s'élevait en 2019 à 1917 milliards de dollars, soit une augmentation annuelle de 3,6 % par rapport à 2018, la plus forte depuis 2010. Cinq Etats ont dépensé le plus en 2019 et concentraient 62 % des dépenses : Etats-Unis, Chine, Inde, Russie, Arabie saoudite. Pour la première fois, deux Etats asiatiques figurent dans le tiercé de tête. En Europe et contrairement aux idées reçues, les dépenses militaires de la première puissance économique de l'Union européenne, l'Allemagne, ont augmenté de 10 % en 2019, pour atteindre 49,3 milliards de dollars. Il s'agit là de la plus forte augmentation des dépenses des 15 Etats qui dépensaient le plus pour leurs forces armées en 2019. En comparaison, la Suisse dépense pour sa défense moins de 1 % de son PIB. Depuis 1960 où il se montait à 2,7 % (avec prise en compte des prestations APG), ce pourcentage se trouve en nette baisse depuis la fin de la guerre froide[3]. L'armée 61 appartient bel et bien au passé. Dans le climat actuel d'incertitudes liées à la fois à la situation internationale, aux prochaines élections présidentielles américaines, au dérèglement climatique et, *in fine*, à l'évolution de la pandémie, il est prématuré de prédire une baisse générale des dépenses militaires,

2 SIPRI, Military Expenditure Database : https://www.sipri.org/databases/milex (lien actuel)

3 Professeur Cédric Tille, « L'armée est-elle un boulet financier ? », *L'Agefi,* 11.08.2020 : https://www.agefi.com/home/acteurs/detail/edition/online/article/larmee-est-elle-un-boulet-financier-498279.html (lien actuel)


celles-ci étant liées à la fois à des programmes d'armement



La pandémie du Coronavirus signifie également le retour en force des Etats.

en cours et à des enjeux industriels clé (autonomie stratégique).

**Conséquences pour l'armée suisse (DEVA)**

En Suisse, l'engagement de l'armée au profit des autorités civiles a mis en évidence au moins trois conséquences.
Le modèle d'armée actuel basé notamment sur un fort ancrage régional (via les divisions territoriales) a démontré toute sa pertinence, en particulier par le biais des exercices conduits régulièrement avec les autres acteurs sécuritaires. En France voisine (Auvergne-Rhône-Alpes), un scénario global avait été proposé en septembre 2019, avec implication de tous les services publics. Celui-ci reposait sur l'idée d'une crise majeure qui, en 38 heures, priverait toute la zone de défense considérée de ressources énergétiques et alimentaires. L'exercice devait impliquer des entreprises du secteur des télécommunications, de l'énergie, ainsi que les services de santé et les médias locaux. Jugé non indispensable avant la pandémie, cet exercice est désormais planifié pour l'automne 2020. On peut penser qu'un tel exercice serait pertinent pour nos régions territoriales.

La pandémie ne doit pas faire oublier que la mission principale de l'armée, telle que la Constitution fédérale la formule, reste la défense du territoire et que, pour y parvenir, l'armée doit disposer des moyens nécessaires pour la remplir et, *in fine*, rester crédible. C'est là le prix d'un système de défense dissuasif. A ce jour, personne ne peut préjuger de l'évolution de la situation post Covid-19 (pour autant qu'elle existe) en Europe et dans sa proche périphérie. Dans ce contexte de grande incertitude, un Etat neutre ne peut compter que sur ses moyens et ne pas spéculer sur une hypothétique coopération avec des Etats étrangers.

En situation d'urgence, qu'il s'agisse d'une pandémie ou d'une menace terroriste, la première ligne de défense du pays reste son renseignement. Celui-ci permet aux autorités de conserver une vue globale et indépendante de la situation, dans un monde où l'abondance d'informations tend à tuer l'information et à alimenter les fausses nouvelles (« fake news »).

SRM

Pendant la pandémie, les informations transmissent par les organes nationaux et internationaux n'ont pas toujours été vérifiables ou valides.

*Renseignement*

## Les défis du renseignement d'origine de sources ouvertes pendant la pandémie du coronavirus

**Sean Cordey*, Marie Baezner ****
* Chercheur au Cyber Defense Project, Center for Security Studies (CSS)
** EPFZ, Collaboratrice scientifique,

Tout comme la société en général, la pandémie du coronavirus a aussi bouleversé la communauté du renseignement occidental. Elle a généré une nouvelle demande pour ce que beaucoup nomment « le renseignement de santé publique » – un mandat que beaucoup d'agences de sécurité et de renseignements n'avaient, en réalité, jusqu'à là, pas ou peu considéré comme part de leur mandat (hormis le Med Intel).[1] La mission du renseignement est ainsi devenue double : surveiller et analyser l'évolution, la transmission et les implications du virus (à l'interne et à l'externe) tout en luttant contre les menaces « traditionnelles » qui se retrouve amplifiées comme la dés/mal-information, la fraude ou l'ingérence étrangère. Quant à cette première mission, les services de renseignements doivent user de leurs différents outils de collections, comme l'interception de communications (SIGINT), les images satellites (IMINT), les contacts humains (HUMINT), ou encore des informations de sources ouvertes (OSINT).

Dans le contexte du « renseignement de santé publique », les sources ouvertes jouent un rôle essentiel, notamment concernant des systèmes d'alertes, de détection et de suivi des pandémies.[2] Son accessibilité en fait également un outil de choix au-delà du cadre du renseignement. Bien qu'utilisé depuis des années, l'OSINT se retrouve toutefois (re)valorisé depuis plusieurs mois. Dès lors, se pose la question suivante : quels défis et implications pour l'OSINT a présenté la pandémie du coronavirus ? Pour y répondre, cet article introduit dans une première partie l'OSINT avant d'élaborer dans une deuxième partie deux des défis majeurs pour l'OSINT en temps de pandémie avant de conclure en expliquant certaines implications quant à sa (re)valorisation.

### Présentation de l'OSINT

Avant d'élaborer sur les défis et implications de la pandémie sur le renseignement de sources ouvertes, il convient tout d'abord de définir et replacer ce qu'est le Renseignement d'Origine Sources Ouvertes (ROSO) – mais plus communément dénommé « Open Source Intelligence » (OSINT). Concept Americain, on entend par OSINT la collecte, l'analyse et diffusion d'information obtenue à travers des sources d'information publiques (payantes ou gratuites). Du fait de la digitalisation croissante de la société et de la multiplication des médias en tous genres, ces dites sources d'information peuvent être d'une grande variété : télévision, journaux papiers, blogs, sites internet, réseaux sociaux, metadata, imagerie satellite, publications académiques, gouvernementales ou encore commerciales. A l'encontre de la recherche classique, qui a pour but l'acquisition de connaissances, l'OSINT applique des processus et techniques de renseignements dans les buts de recherche d'information dans le cadre d'une tâche spécifique (ex. surveillance journalière des cas coronavirus), de prévenir des menaces et de supporter la prise de décision.

Les services de renseignements – parfois spécialisé comme l'Open Source Center américain – en sont parmi les plus grands utilisateurs, que ce soit pour des motifs de sécurité nationale, de lutte contre le terrorisme et le (cyber)crime ou de renseignement extérieur. L'OSINT n'est pas réservé qu'à ces derniers et pour beaucoup d'autres services gouvernementaux, c'est souvent le seul moyen d'obtenir des informations.[3] Les autorités policières, par exemple, ont recours à la surveillance automatisée des réseaux

1 Wark., W. (2020, Avril 14). *Pandemic gives security and intelligence community and urgent new mission*. Policy Options. https://policyoptions.irpp.org/magazines/april-2020/pandemic-gives-security-and-intelligence-community-an-urgent-new-mission/

2 Loprespub., (2020, Avril 28). *Le renseignement de sources ouvertes et l'alerte rapide en situation de pandémie*. Bibliothèque du Parlement Canadien. https://notesdelacolline.ca/2020/04/28/le-renseignement-de-sources-ouvertes-et-lalerte-rapide-en-situation-de-pandemie/

3 Center for Security Studies, (Avril 2008). *Open Source Intelligence: nouveau paradigme du renseignement?*. Politique de sécurité : analyses du CSS. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysen-32-FR.pdf

sociaux ou des programmes de reconnaissances faciales comme *Clearview AI*.[4] Similairement, les organisations internationales comme l'ONU ou la Croix-Rouge utilisent l'OSINT pour soutenir et sauvegarder leurs diverses opérations. Le secteur commercial en est également friand – si ce n'est plus que le secteur public – notamment dans le cadre de l'étude de nouveaux marchés, la surveillance de la concurrence, la planification marketing ou la lutte contre les cyber-risques. On retrouve également toute un écosystème proposant des services d'OSINT pour des tiers (ex. Oxford Analytica ou L'Economist Intelligence Unit). Finalement, l'OSINT est aussi employé comme technique de reconnaissance par des acteurs malicieux, que ce soit des hackers, criminels ou terroristes.

Comparé aux autres moyens de collecte de renseignements, l'OSINT présente un certain nombre d'avantages. Tout d'abord, il ne présente aucun risque réel. De plus, il est généralement moins coûteux, ne nécessitant pas d'équipements sophistiqués (ex. des bases SIGINT ou satellites espions). Les informations accessibles au public sont non seulement faciles d'accès, mais peuvent en outre être recueillies par un cercle d'analystes décentralisés et d'utilisateurs potentiels beaucoup plus grand. A cela s'ajoute le peu de contraintes juridiques et de confidentialité qui encadre la collecte et la diffusion de ces renseignements.

**Pandémie coronavirus : les défis pour l'OSINT**

De manière générale, le ROSO doit faire face à de nombreux défis, les plus importants étant : 1) le volume toujours plus croissant de données et d'informations accessibles ainsi que 2) la fiabilité des sources et informations collectées. Bien que la pandémie ait ouvert la voie à de nombreuses applications et opportunités dans le domaine de l'OSINT, elle a également considérablement accentué ces deux défis.

*1) Volume gargantuesque de données et d'information : une question de triage et de pertinence.*

Tout d'abord, le confinement général des populations a eu pour conséquence une augmentation de l'usage des divers solutions et services numériques (ex. réseaux sociaux, programme de téléconférence, journaux en ligne, le cloud, sites de streaming, …) que ce soit pour des raisons professionnelles, personnelles ou de divertissement. Le résultat a été une véritable hausse de la demande/génération de données. Les statistiques sur l'utilisation de l'internet en témoignent : à la mi-mars 2020, le centre d'échange internet DE-CIX basé à Francfort - le plus important au monde en termes de trafic de données - a signalé une augmentation de 60 % du traffic (4.2 à 6.8 Térabit (Tbit) par secondes) entre mars 2019 et mars 2020, avec un pic 9.1 Tbit à la mi-mars.[5] Ce niveau record est la plus forte augmentation du trafic de données que la société n'ait jamais enregistré. De leurs côtés, les plateformes de médias sociaux ont aussi connu une forte hausse d'utilisation. Facebook, par exemple, a signalé en mars une augmentation de 50 % des messages dans les pays les plus touchés par le virus.[6] Indiquant que les personnes qui se tenaient auparavant à l'écart des médias sociaux se sont progressivement tournées vers ces plateformes pour s'informer et échanger avec leurs proches – une « habitude » qui généralement perdure une fois prise.[7]

En outre, une pléthore d'informations (tous formats compris) sur la crise sanitaire – ex. rapports officiels et commerciaux, nouvelles, livres… – ont été rendu accessibles au public. Cela est dû à la demande croissante de besoin d'informations des populations, qui a résulté sur une communication de crise constante, institutionnalisée et ritualisée (ex. le nombre d'infections, les mesures de confinement ou les listes rouges). Par logique économique, le secteur privé a également répondu à cette demande en mettant à disposition ses services et informations. En effet, compte tenu de la sensationnalisation de la crise, beaucoup de journaux online ont partiellement abaissé leurs « murs de paiement » (paywall) relatifs à la pandémie. Mesures qui viennent s'ajouter aux dynamiques informationnelles et politiques préexistantes comme le cycle d'information constants ou la décentralisation des sources informationnelles. Au-delà des médias, d'autres acteurs économiques, notamment dans le « Big data », le consulting, l'intelligence économique ou sécuritaire ont capitalisé sur la crise pour vendre leurs produits.

La hausse de la demande et génération de données et d'informations ont créé de nombreuses opportunités d'OSINT à des fins de traçage de la pandémie. Parmi les usages, on y retrouve par exemple, en mars, l'analyse du soudain ralentissement de l'Internet Malaysien qui a laissé entendre une situation sur place pire que les 129 cas alors annoncés.[8] De même que la surveillance d'Internet en Chine tout au long de la pandémie a montré comment les usines industrielles des régions les plus touchées se sont arrêtées pendant l'épidémie avant de reprendre, donnant de cruciales informations sur la situation sur place. Ou encore, les données de TomTom sur le trafic routier de diverses villes chinoises et italiennes ont servi à comprendre comment elles étaient affectées par les quarantaines et les restrictions de mouvement.

4 A noter que les abus sont nombreux et que les techniques ne sont pas toujours au points. Pour rappel, les émeutes de 2015 à Baltimore trouvent entre autre leurs origines dans des messages sur les réseaux sociaux mal interprétés par les forces de l'ordre.

5 DE-CIX, (2020, Mars 11). *Highest jump ever: DE-CIX Frankfurt reaches 9.1 Tbps*. https://www.de-cix.net/%20de/news-events/news/de-cix-frankfurt-reaches-9-1-tbps.com ; De-CIX., (2020 Septembre 11). *Frankfurt Statistics*. https://www.de-cix.net/en/locations/germany/frankfurt/statistics

6 Schultz, A. & Parikh, J., (2020, Mars 24). *Keeping Our Services Stable and Reliable During the COVID-19 Outbreak*. Facebook. https://about.fb.com/news/2020/03/keeping-our-apps-stable-during-covid-19/

7 Blackdot. (2020). *How Covid-19 will impact the use of OSINT*. Blackdot solutions. https://blackdotsolutions.com/osint-covid-19/

8 Volpicello, G., (2020, Mars 20). *Hidden Data is revealing the true scale of the coronavirus outbreak*. Wired. https://www.wired.co.uk/article/coronavirus-spread-data


La dés/mal-information relatant à la pandémie fut rampante et compliqua l'évaluation des sources.

Malgré ces bienfaits, l'explosion et le trop-plein de données et d'informations est également un des défis majeurs pour l'OSINT. En effet, selon Travis Wright, aujourd'hui « *les dirigeants et les organisations ne cherchent plus des aiguilles dans les meules de foin, ils cherchent des aiguilles spécifiques dans des montagnes d'autres aiguilles* ».[9] En effet, la collecte de l'OSINT produit et brasse une grande quantité de données et d'informations qui doivent être fastidieusement triées, filtrées et analysées – à temps – pour être considérées comme utiles et pertinentes. Il existe de nombreux outils automatisés à cette fin, et de nombreux gouvernements et entreprises ont développé leur propre ensemble d'outils et de techniques d'intelligence artificielle pour filtrer les données collectées. Mais de telles informations ne peuvent souvent être vérifiées et questionnées qu'avec des outils de renseignement traditionnels et la « touche humaine ». En effet, il est souvent nécessaire de visualiser et comparer avec certaines données classifiées les résultats des outils automatisés pour s'assurer de leur fiabilité et de leur pertinence – opération chronophage et qui nécessite des ressources humaines. Ce processus a été d'autant plus compliqué lors de cette pandémie, car beaucoup de services de renseignements ont été contraints à une importante réorganisation pour éviter de propager la maladie dans leurs rangs, impliquant parfois une perte d'accès à certains servers ou contacts humains.

Fiabilité des sources : dés/mal-information, dépassement des institutions nationales et internationales et processus académique en marge.

Le deuxième défi majeur pour l'OSINT est la fiabilité des sources et la véracité des informations, notamment dans un contexte ou 1) la dés/mal-information est rampante, 2) les institutions nationales et internationales sont dépassées ou peu fiables et 3) les processus de création de savoir académique fiable sont minées.

La pandémie a vu l'augmentation massive des volumes de données échangés sur Internet – contenus officiels ou officieux, confidentiels ou ouverts, exacts ou faux[10] –

9 Wright, T. (2020, Mars 19). *The value of Open Source Intelligence in a Pandemic Environment*. RealClearDefense. https://www.realcleardefense.com/articles/2020/03/19/the_value_of_open_source_intelligence_in_a_pandemic_environment_115131.html

10 24heures. (2020, Mars 23). *Covid-19* :un défi aussi pour les services


L'anxiété et l'incertitude générale ont contribué à une augmentation de la demande et production de données et d'informations, compliquant le travail des analystes d'OSINT tout en leurs offrants de nouvelles opportunités.

générant une « infodémie » dans laquelle de nombreux acteurs tentent d'avancer leurs pions stratégiques, économiques ou politiques. Parmi ces acteurs, l'on retrouve notamment des états (ex. la Chine, la Russie, l'Iran, Israël mais encore les Etats-Unis) qui ont déployé des stratégies d'influence ambigües, voire agressives pouvant utiliser des informations inexactes ou tronquées afin d'avancer divers intérêts dont : le contrôle du narratif autour de la pandémie (ex. la gestion et origines de la pandémie); la perturbation des efforts adverse de lutte contre la pandémie (ex. en augmentant la panique locale ou en réduisant la confiance dans les institutions) ; ou encore comme tremplin pour de l'espionnage économique, politique, ou médical – notamment concernant les chiffres d'infections et la recherche sur les vaccins (ex. par le biais de « Phishing »). S'ajoute une multitude d'acteurs non-étatiques, comme les cybercriminels, les complotistes ou les groupes politiques extrêmes, qui ont – sciemment ou non – diffusés de fausses informations. Parmi la légion d'exemples, citons la question des traitements (ex. l'hydroxychloroquine ou javel), des mesures d'urgence (ex. l'établissement de la loi martiale en Angleterre ou l'instrumentalisation du confinement pour faire taire les Gilets jaunes) ainsi que des complots (ex. l'invasion de l'Europe par les Etats-Unis – cf. « Defender 2020 »).

Tous ces acteurs ont profité, exploité et parfois contribué à un contexte propice à la multiplication des fausses informations. Un contexte qui se définit notamment par un climat généralisé d'isolement, d'incertitude, d'instabilité et de grande anxiété qui a résulté en une demande croissante d'information. Notons aussi une plus grande dépendance et utilisation des réseaux sociaux pour s'informer – renforcée pendant le confinement ainsi qu'une grande accessibilité et maturité des produits et techniques de « cyber influence » (ex. bots, faux comptes …). Tout cela dans un climat international et national parfois délétère, polarisé et divisé qui prête à l'abus et l'ingérence.

En plus de la dés/mal-information rampante, mentionnons que les institutions nationales ou internationales qui dirigeaient l'essentiel des efforts contre la pandémie n'ont pas toujours été en mesure de transmettre des informations valides et vérifiées. A l'échelle nationale, de nombreux pays ont délibérément caché et menti sur la situation réelle dans leur pays (ex. Chine et Iran). Alors que les différentes pratiques (parfois régionales) de collecte et de comptage ont rendu beaucoup de ces données suspectes ou simplement erronées – comme ce fut notamment le cas en Suisse lors du chiffrement des infections dues aux boîtes de nuits.[11] A cela s'ajoute aussi le manque de moyens, de préparation, d'entrainement et de coordination au sein même des états et administrations. Dans le cas de la Suisse, on ne peut que penser aux fameux fax des chiffres journaliers de l'OFSP de mars dernier.[12]

Quant au manque de coordination et de vision, le brigadier Raynald Droz – Chef d'état-major du commandement des Opérations – avançait en mars que : « l*a plupart d'entre nous – hormis les membres de notre cellule MedIntel – pensions que cela [la situation sanitaire en Chine] ne nous concernerait pas directement.* »[13] A l'échelle internationale, les informations publiées par certaines institutions intergouvernementales ont également été grandement décriées pour leur manque de précision ou leur arrivée tardive. L'OMS est sans doute l'exemple le plus notable : beaucoup d'experts et d'officiels lui ont reproché d'être sous l'influence du pouvoir chinois ainsi que son manque de transparence et la gestion de la

de renseignement. 24 heures. https://www.24heures.ch/monde/covid19-defi-services-renseignement/story/12259636

11 OFSP, (2020, Aout 2). *Rectification: les lieux de contamination sont les contextes familiaux et non les boîtes de nuit.* https://www.bag.admin.ch/bag/fr/home/das-bag/aktuell/news/news-02-08-2020.html

12 RTS info. (2020, Mars 18). *Les annonces de nouveaux cas de coronavirus se font par fax.* RTS. https://www.rts.ch/info/suisse/11175710-les-annonces-de-nouveaux-cas-de-coronavirus-se-font-par-fax.html

13 Chevillot, A., & Roten, N. (2020, Mars 24). *Coronavirus : « Si quelqu'un avait voulu fomenter un acte radical, réfléchi et très efficace, il ne s'y serait pas pris autrement ! ».* Heidi.news. https://www.heidi.news/sante/coronavirus-si-quelqu-un-avait-voulu-fomenter-un-acte-radical-reflechi-et-tres-efficace-il-ne-s-y-serait-pas-pris-autrement

pandémie.[14] En effet, avant de tardivement déclarer que la pandémie était une « Urgence de santé publique de portée internationale », l'OMS aurait répété sans critiques les informations des autorités chinoises tout en ignorant les avertissements des médecins taïwanais. Ceci, ajouté aux multiples aller-retours concernant la nécessité de porter des masques ou non, a considérablement affecté la crédibilité des informations publiées, donc par ricochet celle des institutions.

Alors que le statut de la science est déjà en train de s'éroder, un dernier élément contribuant à la difficile vérifiabilité des sources ouvertes a été la diffusion généralisée et le recours à des sources académiques souvent problématiques. En effet, de par la nouveauté du sujet d'étude et les fonds considérables qui ont été débloqués pour la recherche, il y a eu une course à la publication et à l'attention, souvent au dépens de la rigueur académique (ex. méthodologie et examen par les pairs) et médicale (ex. aveugle, double aveugle, randomisée) – l'on pense notamment à ces études sur l'hydroxychloroquine qui n'étaient pas randomisées. Compte tenu d'un processus de recherche académique médical – traditionnellement long – la grande majorité des études qui sont publiées ne sont que des pré-études dont les résultats ne doivent pas toujours être pris pour vrai et doivent encore être vérifiés – une distinction que le grand public ne comprend pas toujours. A cela s'ajoute le fait qu'il existe également un pan de la littérature qui provient de pseudo journaux/revues académiques aux tendances prédatrices.[15] Sous couvert de simili authenticité, ces revues publient – contre une rémunération – toutes sortent d'articles sans aucune forme de test de qualité.

## Conclusion

La pandémie du coronavirus n'a que renforcé l'utilité et la nécessité des services de renseignements de considérer l'OSINT comme une branche à part du renseignement.[16] En effet, l'OSINT complète pleinement d'autres types de renseignements grâce au « cross-intelligence ». Essentiel, il permet de complémenter et affiner la compréhension et la connaissance d'une cible d'intérêt et de son environnement, notamment pour l'analyste.[17] Il peut même parfois compenser – jusqu'à un certain point – certaines autres méthodes de renseignement qui se trouve limitées conjoncturellement (ex. l'HUMINT pendant la période de confinement) ou financièrement.

Dans le cadre de la santé publique, en particulier, l'OSINT s'est révélé avoir un important potentiel, particulièrement concernant les systèmes de suivi, de détection et d'alerte précoce. Pour preuve, depuis quelques mois, de nombreuses initiatives en tous genres ont vu le jour – ex. *l'Epidemic Intelligence from Open Source* (EIOS) de l'OMS – ou ont été relancée – ex. *Global Public Health Intelligence Network* du Canada.[18] Ces initiatives et la (re)valorisation de l'OSINT font suite à la réalisation de certains « manquements » – que certains ont qualifiés de « défaillance/échec de renseignement » bien que beaucoup d'experts au sein des divers services de renseignements et agences spécialisées en signalaient les risques depuis des années. Ces dites « défaillances » sont en train de favoriser – comme aux Etats-Unis après le 11 septembre et la guerre en Irak – un réexamen approfondi de la manière dont les informations sont recueillies, analysées et utilisées dans le cadre de la prise de décision. A cela s'ajoute la volonté de certains gouvernements de développer leurs propres compétences dans le domaine pour ne plus dépendre de l'OMS (qui a perdu en crédibilité) ainsi qu'assurer le suivi stratégique et sécuritaire. A cet effet, ce développement ne fait que s'inscrire dans une plus grande dynamique d'(hyper) sécurisation de plus en plus de domaines de nos sociétés. Dynamique qui fait suite à l'élargissement des menaces sécuritaires – et donc mandat des instances de sécurités – depuis la fin de la guerre froide. Après l'environnement, c'est à présent la santé qui se retrouve à nouveau au centre de l'attention de l'appareil sécuritaire.

Pour conclure, malgré la (re)valorisation apportée par la pandémie, l'OSINT ne doit pas être vue par les services de renseignements comme une solution miracle. L'OSINT fait face à des défis – quantité de données et la véracité/vérifiabilité de celles-ci – difficilement surmontables seuls, particulièrement lorsque les organes de renseignements manquent de ressources et d'expertise dans certains domaines (ex. épidémiologie). Dans ce dernier cas, l'expertise pourrait être d'avantage internalisée ou captée au sein des communautés académiques et scientifiques.[19] Il n'empêche qu'il est critique que les services de renseignement développent leurs capacités et connaissances en matière d'OSINT. Non seulement pour répondre à leur mission qui va encore évoluer, mais aussi pour faire face à la grandissante monétisation et privatisation du secret – et donc une fragilisation du monopole du renseignement et *l'ultima ratio* des Etats – menées par les géant américains et asiatiques de la Tech et du web.[20]

S. C. & M. B.

14 Feldwisch-Drentrup, H. (2020, Avril 2) *How WHO became China's Coronavirus Accomplice*. Foreign Policy. https://foreignpolicy.com/2020/04/02/china-coronavirus-who-health-soft-power/

15 RTS. (2020 Aout 8). *Des revues scientifiques prédatrices qui publient n'importe quoi*. https://www.rts.ch/play/radio/cqfd/audio/des-revues-scientifiques-predatrices-qui-publient-nimporte-quoi--les-mollusques-suisses-la-personnalite-des-insectes?id=11534447

16 Charon, P., & Laurencon, F. (2020). *Les nouveaux enjeux du renseignement*. Le Figaro Enquêtes.

17 *Ibid.*

18 Le Canada est en train de mener un audit pour déterminer les causes de sa fermeture par le gouvernement entre Mai 2019 et Août 2020.

19 Charon, P., & Laurençon, F. (2020). *Les nouveaux enjeux du renseignement*. Le Figaro Enquêtes.

20 *Ibid.*

Jean-Baptiste Bless est au Sahel depuis plus de 4 ans. Après avoir été analyste au sein de l'Etat-major 1 de la MINUSMA, il est devenu Conseiller sécurité pour les représentations suisses en Afrique de l'Ouest. Ses analyses sont émises à titre privé et n'engagent que lui.

*Renseignement*

# Mali : un coup d'Etat pour un nouveau départ ?

**Jean-Baptiste Bless**
Conseiller sécurité pour les représentations suisses en Afrique de l'Ouest

Le 18 août passé a eu lieu à Bamako, capitale du Mali le 4e coup d'Etat depuis l'indépendance du pays en 1960. Or, si le terme « coup d'Etat » est en principe associé à la violence et à la soif de pouvoir, il s'est, en l'occurrence, déroulé sans effusion de sang et a débouché sur une transition civile. On ne peut donc pas parler de « putsch ». Ce fut un coup d'Etat « en douceur », et il vaut donc la peine de se pencher sur les circonstances particulières, bien éloignées de nos réalités helvétiques, pour en tirer quelques leçons.

## Contexte et réactions

Ce 4e putsch rappelle celui de 2012, mais a été mieux pensé et préparé, sans doute en tirant les leçons du dernier. Ce genre d'action n'est pas une spécificité malienne, puisque, pour ne prendre que la dernière décennie, le voisin nigérien a connu des événements similaires en 2010. L'autre voisin sahélien, le Burkina Faso, a également vécu une tentative de coup d'Etat en 2015, les militaires échouant cette fois-ci à reprendre le pouvoir après l'insurrection de 2014. « Insurrection populaire » et « action militaire » : ces deux éléments se retrouvent dans les événements d'août 2020 au Mali, nous y reviendrons. Mais notons déjà le rôle récurent des armées dans les transitions politiques du Sahel.

Les réactions venant de puissances étrangères ont été en décalage flagrant avec la liesse populaire qui a accueilli les militaires : les condamnations furent quasiment unanimes, avec pour seul mot d'ordre le « retour à l'ordre constitutionnel ». La France, pragmatique de par sa présence multi-faciale dans la région, a, dans un second temps, adopté une position plus nuancée avec une référence à « l'intérêt du peuple malien ». Quant aux Etats-Unis, ils ont parlé de « mutinerie » et non de « coup d'Etat », histoire de ne pas devoir interrompre leur coopération. La réaction la plus épidermique est venue de la CEDEAO,[2] communément décrite par la presse africaine comme un « club de chefs d'Etats ». Ces derniers n'ont jusqu'à ce jour pas relâché la pression sur le pays, lui imposant de lourdes sanctions afin de peser dans les négociations : la libération du Président, un retour rapide à l' « ordre constitutionnel », une transition courte et dirigée par un civil, etc. Le rôle traditionnel de cette institution régionale s'explique entre autres par la crainte que partagent certains présidents de subir un sort similaire. Notons tout de même qu'ils ont rapidement dû abandonner leur première revendication, à savoir le retour du Président déchu Ibrahim Boubakar Keita (IBK), ce dernier ayant confirmé sa « démission ».

## Déroulement des évènements

Que s'est-il réellement passé à Bamako le mardi 18 août ? Au matin, la ville se réveille au son de coups de feu en provenance du camp militaire de Kati, et les premiers rapports parlent d'une mutinerie. Puis des rumeurs courent sur l'arrestation de certains ministres, la prise de contrôle de la radio d'Etat, l'ORTM, et du palais présidentiel. Le soir, on apprend qu'une junte composée de cinq jeunes colonels a pris le contrôle de la machine d'Etat et effectivement arrêté les principaux ministres, ainsi que le Président IBK. Ce dernier apparaît le soir même à l'écran et annonce sa démission, après avoir signé la dissolution du gouvernement et de l'Assemblée nationale.

Comment une action si imprévue a pu atteindre son objectif si rapidement ? Sans doute grâce à une bonne préparation. L'histoire dira si les protagonistes ont bénéficié du soutien d'une puissance extérieure ; notons en tous les cas que la plupart des membres de la junte bénéficient d'une formation en France, en Russie ou aux Etats-Unis. Précisons également pour simplifier que le fruit était mûr : la contestation épisodique de la rue depuis la réélection d'IBK en 2018 était devenue

régulière et de plus en plus intense depuis les élections législatives de juin dernier et la mise en place par la Cour constitutionnelle de candidats proches d'IBK. De plus, le président était accusé depuis longtemps de népotisme, de détournements de fonds et de mauvaise gestion des affaires, notamment de la situation sécuritaire au Nord et au Centre du Mali. Selon les termes même de l'opposition politique, regroupée sous le parapluie du M5-RFP, les militaires ont « parachevé la lutte du peuple malien » en apportant le coup de pouce à un processus engagé de longue date. Y a-t-il eu unanimité à l'intérieur du pays ? Difficile à dire, mais seuls les institutions inféodées à IBK, telles que l'Assemblée nationale et la Cour constitutionnelle, ont protesté, avant de se faire emporter par les évènements. Cette convergence ponctuelle des forces populaires et militaires laisse penser que les historiens parleront peut-être de « révolution » ou de « printemps malien ».

Mentionnons que les militaires ont également géré la suite des événements de manière responsable, puisqu'ils ont immédiatement confirmé vouloir se tenir aux accords internationaux, avant d'inviter la population à arrêter ses pillages et les services de l'Etat à poursuivre leurs activités dans le calme. Ils ont communiqué de manière adroite, indiquant qu'il n'y avait pas eu de coup d'Etat, mais que le Président avait été « mis en sécurité », ce qui n'était pas loin de la réalité au vu de la colère populaire. Ils se sont également préoccupés des formes légales, s'assurant qu'IBK dissolve les principales institutions de l'Etat. Il n'est pas à exclure que le président ait été soulagé de la tournure des événements étant donné l'impasse dans laquelle il se trouvait et son état de santé préoccupant. En tous les cas, il semblerait que les principes généraux de la conduite tactique aient été respectés, en particulier : simplicité, sûreté, surprise. Concentration et économie des forces pour un résultat atteint sans coup férir : un exemple du genre, malgré les réserves légalistes qu'on peut avoir

**Quelques éléments de réflexion**

D'un point de vue constitutionnel, le rôle joué par l'armée mérite attention : l'équilibre entre les pouvoirs (législatif, exécutif et judiciaire) n'ayant pas fonctionné, le pouvoir militaire en tant que 4e pilier de l'Etat vient remettre les compteurs à zéro. Ce phénomène de balancier entre un pouvoir civil à tendance autocratique et un pouvoir militaire (provisoire ou durable) semble une constante des pays de la région et doit répondre en partie à des spécificités culturelles. Précisons toutefois que les régimes autoritaires tenus par des militaires tendent à disparaître et que la rue a pris du poids, les gouvernements étant de plus en plus réticents à engager la force, et les réseaux sociaux favorisant les mouvements populaires d'envergure. Dans notre cas, la convergence des colères populaires et militaires est particulièrement intéressante, les uns ayant poussé – à leur insu - les autres à l'action décisive. On assiste à une forme de légitimation par les faits, mais nous laisserons les constitutionnalistes débattre de façon plus pointue sur les rapports entre « légalité » et « légitimité »…

Le Président IBK annonce sa démission.

L'action de l'armée est aussi explicable par les frustrations accumulées en son sein : fraudes sur les contrats d'achat et d'entretien du matériel, mauvaise paie et double comptabilité avérée des salaires des soldats, enrichissement éhonté de certains généraux, mais surtout : désintérêt de l'appareil politico-militaire pour la condition du soldat sur le front, avec pour résultat des morts à répétition que ce soit à travers des attaques de convois ou de bases militaires. Or les vrais responsables de ces morts sont les politiques et les généraux, incapables de donner à leur armée les moyens de se défendre et de reprendre le contrôle du territoire, et ce malgré des budgets exorbitants sur le papier. Peut-on reprocher à l'armée de se faire justice quand celle-ci est bafouée et au prix du sang de ses soldats ?

En parallèle, ces mêmes soldats font l'objet de l'opprobre internationale lorsque, dans leur exaspération, ils dérapent et commettent des exactions sur les populations civiles, parfois complices des groupes djihadistes. Nombreuses sont en effet les voix des ONG qui s'élèvent pour dénoncer les exactions – professionnellement et moralement inacceptables, à n'en point douter, mais rares sont celles qui proposent des soutiens à ceux qui, pourtant, accompagnent les convois officiels de délégations étrangères, quand ils ne sécurisent pas ce que le jargon appelle les « couloirs humanitaires ». Position ambigüe des acteurs internationaux, donc, dont la junte devrait se souvenir.

Il est courant d'entendre dans les milieux diplomatiques et humanitaires au sens large que la solution à la crise pluridimensionnelle qui secoue le Mali ne peut pas être uniquement militaire, et c'est une évidence. Mais ce constat récurrent révèle, outre la faiblesse de l'armée malienne et les limites de l'opération française Barkhane, l'impuissance des autres acteurs sur le terrain : gouvernement malien, mais aussi puissances internationales, missions onusiennes, acteurs de développement, ONG de toutes sortes, etc. L'occasion est unique pour faire un bilan et réfléchir en détails les différentes stratégie. Cependant, si c'est du peuple malien lui-même que doit émerger un jour un quelconque sursaut, reconnaissons que l'armée y aura apporté sa part en tant que fer de lance de ce mouvement.

La junte s'exprime à travers son Président, le Colonel Goïta (en beige).

**Et maintenant?**

Mais l'histoire ne fait que commencer. Avec Bah N'Daw comme Président de la transition, la junte a choisi un homme réputé pour son intégrité: militaire à la retraite, mais également ancien ministre, il semble avoir la stature morale et l'expérience pour s'attaquer aux nombreux chantiers qui l'attendent: sécurisation du territoire, lutte contre la corruption systémique, réforme des institutions de l'Etat, soutien aux régions périphériques délaissées,[3] relecture de l'accord de paix, pour ne nommer que les principaux. La remise à plat des principes de fonctionnement de l'Etat malien offre également l'occasion aux bailleurs de fonds internationaux, dont la Suisse, de revoir leur stratégie dans le pays pour ne pas répéter les mêmes erreurs. La période de transition, qui a commencé fin septembre et doit durer 18 mois, apportera certainement encore son lot de surprise; le résultat de ce temps de gestation sera à la hauteur de la capacité des différents acteurs à se remettre en question. ; au prix, pourquoi pas, d'une deuxième déclaration d'indépendance du peuple malien.

J-B. B.

1 Mission multidimensionnelle intégrée des Nations unies pour la stabilisation au Mali

2 Communauté économique des Etats de l'Afrique de l'Ouest

3 La décentralisation à la française ayant échoué, peut-être serait-il temps pour ce pays multi ethnique d'envisager un système fédéraliste ?

Parabole de la déception.

*Renseignement*

**Nos états-majors ne sauraient négliger les ruses et la déception!**

**Col Hervé de Weck**
Ancien Rédacteur en chef RMS+

L'Armée suisse n'est pas la seule en Occident qui ne manifeste pas grand intérêt pour les ruses et autres stratagèmes de guerre; ils ne semblent pas faire partie de sa « culture militaire ». Sait-on dans notre pays que Mahomet considérait légitime de mentir dans trois situations: pour réconcilier deux parties à l'occasion d'une discorde, à la guerre et pour apaiser sa femme? Depuis la Seconde Guerre mondiale, les Britanniques s'avèrent des spécialistes en la matière. Ils ont décortiqué les actions de déception des conflits précédents et fait appel à des psychologues, des ingénieurs, des historiens, même des écrivains pour monter de nouvelles opérations de déception. N'oublions pas qu'il existe un principe immuable selon lequel le plus grand nombre croit ce qui est affirmée en premier.

Patrick Manificat, auteur d'un ouvrage très connu sur les expéditions de renseignement en République démocratique d'Allemagne, pendant la Guerre froide, de la Mission militaire française à Berlin et à Postdam,[1] consacre son dernier livre à la déception, ruse, tromperie, camouflage and Co.[2]

## Efficacité

« (...) la duperie a été reconnue presque universellement comme un facteur multiplicateur du succès d'une opération. La déception procure presque toujours à celui qui la met en œuvre des avantages plus importants que prévus et son coût s'avère généralement inférieur à ce qui était initialement planifié, en vies humaines et en argent. Elle distrait relativement peu de soldats des tâches de combat. (...) Les chances pour qu'elles surprennent sont en général de 80 % et les gains de cette surprise sont très élevés. Elle multiplie les chances d'obtenir un succès rapide et décisif. »

Pour ne pas être trompé, il ne suffit pas de tout voir, il faut aussi comprendre, ce qui constitue un défi bien supérieur. Trois techniques de détection des ruses, tromperies et déceptions ennemies permettent d'éviter de mauvaises surprises: par reconstruction, par test de l'incongruité et l'évaluation de la vulnérabilité. La première consiste, dans une situation qui évolue, à distinguer les vrais indices des faux. De trop nombreux analystes négligent de les recueillir tous les deux. Le chiffrage d'une transmission trop rapidement cassé, un camouflage qui remplit mal son office devraient alerter l'analyste. La deuxième permet de voir si le signal émis correspond aux techniques et aux habitudes de l'ennemi. N'est-ce pas trop beau pour être vrai? N'est-ce pas le bruit que nous aurions fait courir si nous avions été à la place de l'ennemi? La connaissance des déceptions utilisées dans le passé permet enfin d'évaluer ses propres vulnérabilités.

Retenons quelques exemples concrets de déception qui débouchent sur une réussite. En automne 1943, les reconnaissances aériennes américaines sur l'île de Rabaul, occupée par les Japonais, montrent de nombreux simulacres d'avions. Le commandement américain s'en sert comme objectifs d'entraînement pour ses bombardiers. En 1944, un appareil en touche un qui provoque une série d'explosions secondaires. Ces leurres gonflables sont en fait des soutes à carburant et à munitions. « FORTITUDE » éloigne 19 divisions allemandes des plages du débarquement de Normandie, pour 1% du coût total des forces d'invasion. 4'500 militaires, dont moins d'un quart appartiennent aux troupes combattantes, soit 0,2 % de l'armée de terre, 0,5 % de la marine et 0,6 % de l'armée de l'air.

En 2009, des insurgés irakiens détournent des images non cryptées d'un drone *Predator*, utilisant le logiciel

1 Manificat, Patrick : *Au cœur de la Guerre froide ; mission militaire de Postdam*. Paris, Histoire & Collections, 2015.

2 Manificat, Patrick: *Qui ruse gagne. Une anthologie de la tromperie guerrière*. Paris, Sophia Histoire & Collections, 2020.

Le largage de poupées-parachutistes sur la Normandie, les 5-6 juin 1944, vise également à le perturber.

En 2009, des insurgés irakiens détournent des images non cryptées d'un drone *Predator*, utilisant le logiciel *Skygrabber* disponible sur le marché pour 26 dollars. Cela leur permet d'identifier les zones peu ou pas surveillées par les Américains. En 1997, le Hezbollah réussit à hacker le retour vidéo d'un drone des forces spéciales israéliennes, il sait ainsi où aura lieu la prochaine opération. Le Gouvernement chinois semble utiliser des drones camouflés en oiseaux pour surveiller la population, de drones-pigeons, tellement réalistes, qu'ils peuvent voler au milieu d'autres oiseaux sans être repérés.

## Toujours de nouveaux moyens

La Direction générale de l'armement français, au début des années 2010, lance le programme bien nommé « CAMELEON », afin de mettre au point un système de camouflage adaptatif pour les blindés. Il prend la forme d'écrans qui habillent le véhicule et se montrent capables d'afficher en direct des motifs qui lui permettent que l'engin se fonde dans son environnement. Une intelligence artificielle interprète les données transmises par des caméras et restitue en temps réel des couleurs proches du paysage alentour, capables de tromper l'œil humain. La technique consiste à recouvrir le blindé de tuiles connectées qui, divisées en pixels, peuvent afficher huit couleurs différentes. Des capteurs enregistrent les couleurs dominantes de l'environnement dans lequel opère le véhicule et transmettent ces informations à un calculateur qui détermine le camouflage le mieux adapté. Mieux encore, en adaptant son rayonnement à la température extérieure, le système est aussi capable de se jouer des caméras thermiques.

Une autre innovation en cours est de recouvrir les flancs d'un blindé avec des modules qui, ayant une structure comparable à celle d'un nid d'abeilles, sont constitués d'éléments pouvant être refroidis ou chauffés très rapidement et contrôlés individuellement. Ainsi, en jouant avec la signature thermique d'un blindé doté d'un tel dispositif, il serait possible de lui faire changer d'apparence pour tromper les capteurs infrarouges. Quant au logiciel RadioMap, testé récemment par les Marines, il permettrait de savoir jusqu'où ne pas aller pour ne pas se faire détecter en visualisant les zones d'émission de brouillage.

« (...) Une autre recherche vient d›être lancée avec le projet *MAGIC*. Pour rendre un véhicule invisible face aux caméras thermiques, ce projet s'appuie sur les propriétés thermochromes d'un matériau à base de dioxyde de vanadium, dont la capacité à émettre des infrarouges change suivant la température. Ces recherches concernent pour le moment la signature infrarouge des véhicules, mais une application pour la tenue des fantassins apparaît possible. Là où une personne habillée normalement apparaîtrait à 37°C sur une caméra, une tenue réalisée avec un matériau spécial pourrait la rendre indétectable en la faisant apparaître bien plus froide. »

## Ruses de guerre

Il faut constamment imaginer des ruses nouvelles, des opérations de déception et ne pas recourir seulement à celles que l'on a apprises, mais en créer soi-même contre ses ennemis, comme les musiciens qui ne ne se contentent pas des mélodies qu'ils ont apprises, mais tâchent d'en composer de nouvelles. Il s'agit d'un véritable apprentissage intellectuel. En plus des règles élémentaires, le colonel Christophe de Lajudie[1] propose cinq procédés qui respectent un principe « Décevoir suppose de savoir qui on peut tromper, ce qu'on veut lui

1 «La déception», réflexions libres à la une de *Militaire*, 17 mars 2018.

cacher et ce qu'on veut lui faire croire ou lui montrer » : Il synthétise ses réflexions en cinq principes :

- Viser à la tête. Il ne faut pas se tromper d'objectif; la déception vise le chef adverse.
- Ne cacher que ce qui peut l'être.
- Aller dans le sens des symptômes du malade. Il est évidemment plus facile de faire croire à l'adversaire quelque chose auquel il croit déjà, ou qu'il espère pour s'y être préparé, que de l'amener à tout changer.

Ne pas écouter son état-major ! Les états-majors ont un défaut universel, ils sont prévisibles. Or décevoir ou surprendre exige d'être imprévisible.

Cohérence, redondance, convergence. Une manœuvre visant à décevoir doit être coordonnée et ordonnée de près dans toutes ses parties.

H. W.

Un des simulacres de Sherman éployés en 1944 dans le sud de la Grande-Bretagne pour induire en erreur le commandement allemand sur le lieu du débarquement...

La veille et l'anticipation technologique permettent une planification des investissements et des développements plus agiles, surtout dans le domaine cyber, où les technologies changent très rapidement.

*Armasuisse S+T*

## La veille technologique au service de l'écosystème fédéral de la cyberdéfense

**MSc Kilian Cuche*, Dr. Alain Mermoud****

* Master of Science HES-SO in Business Administration, orientation Management des Systèmes d'Information

** Chef veille technologique Cyber-Defence Campus, armasuisse S+T

Ces dernières années, on a pu observer une évolution constante des cybermenaces. Elles se développent de manière exponentielle au développement des nouvelles technologies qui apportent des risques mais également des opportunités. Les attaques sont toujours plus sophistiquées et impliquent désormais de l'intelligence artificielle ainsi que des techniques de *social engineering* toujours plus poussées. En fin de compte, l'attaquant a presque toujours une longueur d'avance sur le défenseur qui est constamment sous la pression d'une nouvelle attaque ou d'un nouveau mode de fonctionnement. Les équipes de sécurité sont très souvent en mode réactif, dépendante des actions des attaquants avant de pouvoir prendre des mesures. En effet, une approche *all hazard* (prête pour tous les dangers) impliquerait des coûts beaucoup trop élevés pour les organisations et les Etats.

### Une contribution à la mesure 1 et 2 de la SNPC

Pour faire face à ces nouveaux défis, la cybersécurité s'est énormément développée ces dernières années. Les secteurs publics, privés et académiques redoublent d'efforts pour augmenter le niveau de sécurité et de résilience de la société face aux menaces cyber. La défense dans le domaine cyber est devenue un nouvel enjeu de sécurité nationale. Pour répondre à ces nouvelles menaces, la Suisse a élaboré plusieurs stratégies dont la principale est la stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022[1] (SNPC ou NCS en allemand) qui en est déjà à sa deuxième version. Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a développé son propre plan appelé Plan d'Action Cyberdéfense[2] (PACD) qui est actuellement en révision car il date de 2017.[3] Ces deux documents présentent des mesures à implémenter au sein de l'administration fédérale, mais pas seulement, afin d'augmenter la défense et la résilience cyber de la Suisse.

On constate également que ce domaine est en constante évolution et que les stratégies évoluent avec les menaces, leurs formes et leur intensité. Actuellement, la collaboration entre les différentes entités dédiées au cyber pourrait être améliorée. L'échange d'informations, de connaissances et de compétences est présent, mais pourrait être amélioré et renforcé. La mise en place du nouveau centre national pour la cybersécurité (NCSC) devrait pallier à ce manque une fois qu'il sera totalement fonctionnel.

En partant de ces constats, une thèse de master en systèmes d'information a été réalisée dans ce domaine avec l'ambition d'apporter une pierre à l'édifice de la SNPC et du PACD, et par extension à la cyberdéfense en Suisse.[4]

### Une collaboration CYD Campus, ACAMIL, HES-SO

Ce travail de master réalisé à la Haute école spécialisée de Suisse occidentale (HES-SO) s'est inscrit dans deux projets de recherche appliqués menés par des unités du DDPS impliqués dans la cyberdéfense. Premièrement, la chaire d'économie de défense de l'Académie militaire (ACAMIL) qui a lancé deux projets au sujet de la gestion des ressources (humaines et matérielles) pour la cyberdéfense[5]. Afin de mener à bien ces projets, il était nécessaire de comprendre et connaître l'écosystème public Suisse dédié aux aspects cyber au niveau fédéral.

1 https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie.html

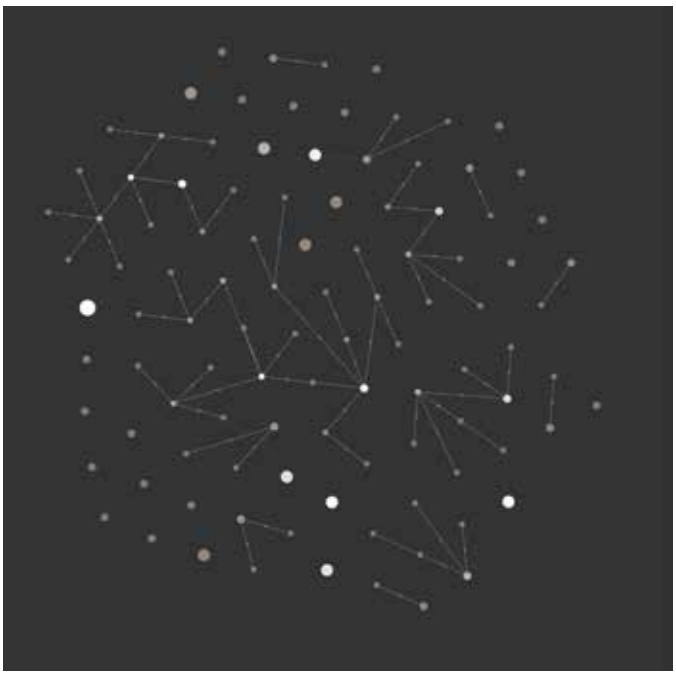
2 https://www.vbs.admin.ch/fr/defense/protection-cyberattaques.detail.document.html/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf.html

4 Cette thèse est disponible sur demande auprès du premier auteur par e-mail : kilian.cuche@vtg.admin.ch

4 Voir article consacré à la chaire d'économie de défense dans ce numéro RMS.

Le deuxième projet dans lequel s'inscrit cette thèse est le développement d'un nouvel outil d'anticipation et de veille technologique (Technology and Market Monitoring 2.0 – TMM 2.0) par le Cyber-Defence Campus basé à l'École polytechnique fédérale de Lausanne (EPFL). Cet outil doit, à terme, servir de soutien à l'anticipation technologique pour tous les acteurs fédéraux impliqués dans le domaine cyber.

Les trois objectifs principaux étaient les suivants. Premièrement, il s'agissait de cartographier de manière interactive les acteurs publics impliqués dans la cyberdéfense au niveau fédéral avec leur mission et leurs compétences pour déterminer qui fait quoi. Ensuite, afin d'aider au développement de l'outil TMM 2.0, une analyse business (compréhension du contexte, des parties prenantes et récolte des besoins des utilisateurs) a été menée parmi les acteurs identifiés. Finalement, une série de recommandations ont été fournies pour le développement de TMM 2.0 afin d'offrir un maximum de valeur ajoutée aux utilisateurs finaux.



Ce graphe en réseau disponible en ligne permet de naviguer entre les différentes unités administratives fédérales impliquées dans le domaine cyber (nœuds) ainsi que de visualiser leurs relations hiérarchiques (arcs).

## Audience cible : les acteurs cyber de la Confédération

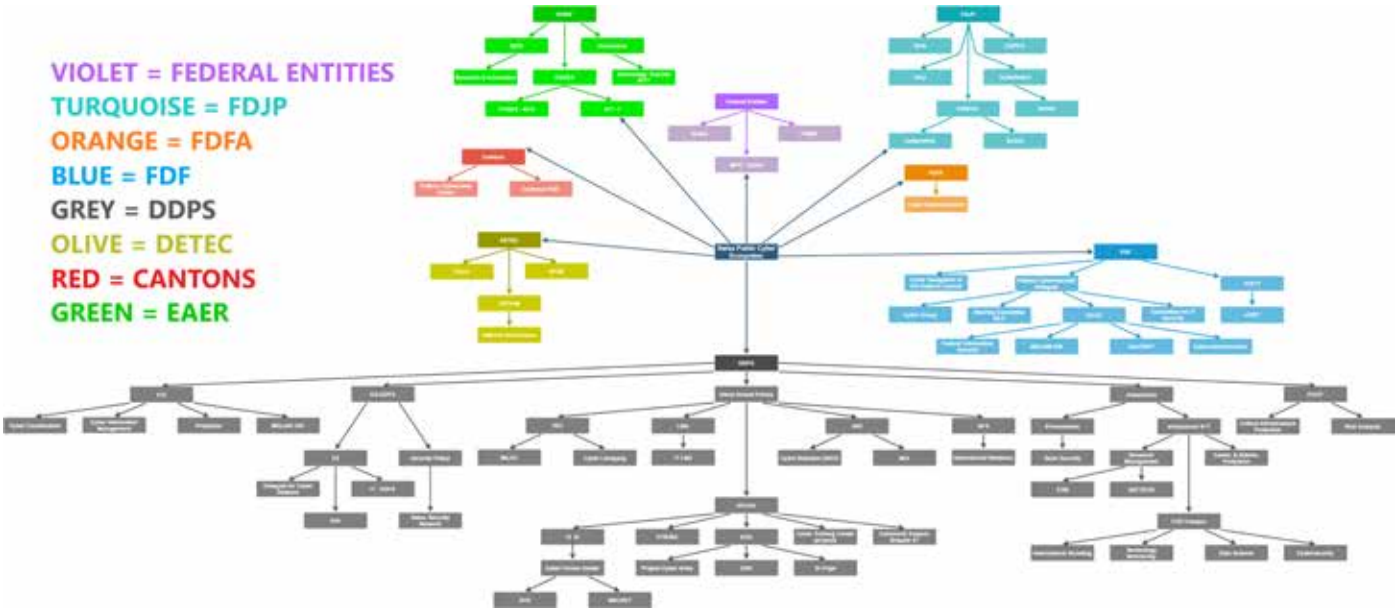
Pour réaliser cette cartographie et identifier les acteurs publics actifs dans le domaine cyber, deux types de données ont été synthétisées. Premièrement, les données *open data* au travers des documents stratégiques de la Confédération et les publications scientifiques et techniques dédiées au domaine cyber en Suisse. Puis, ces éléments ont été complétés par des données qualitatives récoltées au travers d'une quarantaine d'interviews semi-directifs menés avec des acteurs du domaine cyber au sein de l'administration fédérale et du DDPS.

Cet écosystème, considéré comme une organisation, est finalement représenté de deux manières. Premièrement sous la forme d'un graphe en réseau qui représente les relations hiérarchiques entre les unités administratives. L'outil en ligne *Rhumbl* a permis de rendre le résultat accessible pour tout le monde.[6] Cette représentation est vouée à être améliorée et complétée. Toute remarque ou complément sont les bienvenus à l'adresse email mentionnée ci-dessus.

Finalement, cette analyse a également permis de réaliser des tableaux qui présentent et détaillent les activités de 100 entités actives dans le domaine cyber au niveau

6 https://rhumbl.com/app/share/5e8afc1e64f2a64af2d40d47

Cet organigramme disponible sur demande en fichier numérique permet de visualiser l'écosystème fédéral dédié au domaine cyber. Il est séparé par couleurs qui font références aux différents départements de l'administration fédérale.



fédéral. Le graphe en réseau présenté précédemment étant principalement destiné à des analyses pour la recherche, une autre visualisation plus accessible, sous la forme d'un organigramme structurel a également été réalisée.

**Analyse des besoins en veille technologique**

La deuxième phase de cette thèse consistait à analyser les besoins en veille technologique de ces différentes parties prenantes afin d'optimiser le développement de l'outil TMM 2.0. Pour commencer, le contexte du projet a été analysé en collaboration avec les acteurs d'armasuisse Sciences et Technologies (S+T). Ensuite, une analyse de l'outil existant (TMM 1.0)[7] a été réalisée afin de se familiariser avec l'outil et ses capacités.

Finalement, des acteurs externes ont été approchés afin d'avoir une vision de leurs principaux besoins en veille technologique dont par exemple le chef de l'armée, le délégué fédéral à la cybersécurité, les personnes responsables du cyber au secrétariat général du DDPS, le chef de la base d'aide au commandement (BAC), ainsi que le responsable du réseau national de sécurité (RNS). A la fin, ce sont une quarantaine de personnes qui ont été approchées afin de contribuer à l'analyse des besoins pour TMM 2.0.

**Une contribution à la plateforme TMM**

La plateforme TMM est issue d'un projet itératif avec différentes étapes. A la base, TMM était un projet de recherche qui visait à tester des méthodes d'analyse quantitatives pour évaluer l'émergence des technologies en utilisant des informations *open data* comme les publications scientifiques, les brevets et le registre du commerce. En deuxième instance, ce projet a remplacé la base technologique et industrielle importante pour la sécurité (BTIS). Actuellement, TMM permet principalement de rechercher des entreprises en fonction de leurs différentes technologies. Cet outil offre également des analyses sur les tendances technologiques ainsi que des classements d'entreprises, d'organisations et de chercheurs sur des technologies spécifiques. Il est également possible de trouver des brevets, des publications ainsi que des offres d'emploi selon différents secteurs technologiques.

Pour faire suite aux deux stratégies mentionnées en début d'article, le projet TMM 2.0 est né avec pour objectif de répondre aux mesures concernant le développement d'une capacité d'anticipation technologique. Afin de prioriser le développement pour répondre aux besoins principaux, des groupes d'utilisateurs ont été créés afin de pouvoir déterminer leurs besoins essentiels et les représenter sous la forme de produits minimum viables (*MVPs*).

Cependant, avant de déterminer les nouveaux besoins, plusieurs points d'amélioration possible lors du passage de TMM 1.0 à TMM 2.0 ont été identifiés. Ces derniers concernent la définition du cadre et des limitations de l'outil ou encore la différentiation de l'outil par rapport à ses concurrents ou partenaires tel que le programme de prospective technologique DEFTECH. L'augmentation de l'usage ainsi qu'une amélioration des interfaces et des fonctionnalités ont également été relevés. Finalement, il s'agissait d'augmenter la qualité des données et la précision du *crawler* afin de pouvoir délivrer différents scores en toute transparence.

**Recommandations pour TMM 2.0**

Afin de supporter la prise de décision dans la conduite de ce projet, trois types de recommandations ont été proposées. La première concerne la réalisation de *MVPs*. Un *MVP* global présente une priorisation des besoins de tous les utilisateurs afin d'apporter un maximum de valeur lors du développement de l'outil. De plus, les besoins spécifiques de chaque groupe d'utilisateurs sont présentés sous la forme de *MVPs* indépendants. Cette priorisation est réalisée au moyen d'une formule mathématique qui prend en compte l'importance des parties prenantes ainsi que la fréquence du besoin demandé.

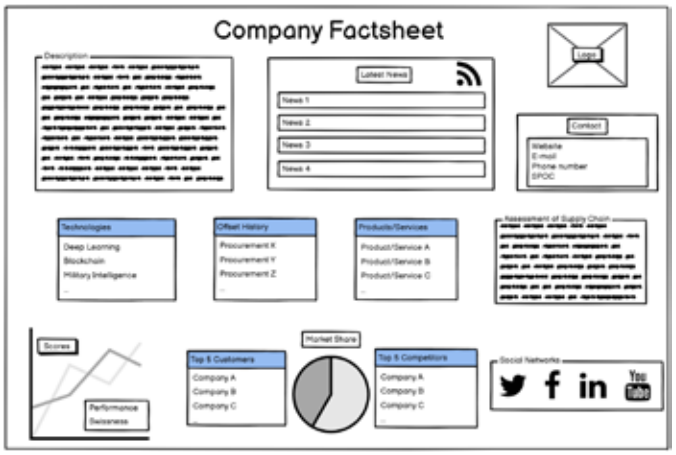
Le besoin principal identifié pour cette plateforme réside dans son approche. Le cadre de recherche doit être international et global au niveau des technologies surveillées. Néanmoins, il est nécessaire d'avoir un focus sur la Suisse afin que cet outil puisse permettre des analyses qualitatives au sein des différentes unités fédérales.

En ce qui concerne les principales fonctionnalités identifiées comme primordiales pour le futur de l'outil, on peut citer la génération de fiches techniques (sur les entreprises et les technologies), la possibilité de s'abonner à des alertes afin d'être averti en cas de changements majeur dans le paysage technologique ou le marché de la défense ainsi que l'accès à des rapports sur mesure centrés sur une technologie ou une entreprise particulière.

La visualisation des données prend également une place importante, que cela soit sous la forme de tableaux de bord stratégiques ou de *hub* d'export de données pour les chercheurs. Finalement, des nouvelles possibilités de filtres ont été demandées (actuellement, le seul filtre disponible est celui des types de technologies) comme des filtres par secteur d'activité basé sur la nomenclature générale des activités économiques (NOGA), par capacité militaire ou encore par région, pays et date.

L'outil devra être capable d'intégrer des sources internes ainsi que des données non-structurées tout en disposant d'une interface utilisateur agréable et moderne (*responsive*). Concernant la transition de TMM 1.0 vers TMM 2.0, certains points d'importance ont relevés tels que l'intégration et la communication avec les parties prenantes tout au long du processus ainsi que la possibilité de former les potentiels utilisateurs sur l'outil. Finalement, la classification des informations aura une énorme importance suite à la possible intégration de sources internes. Il s'agira de bien gérer les droits d'accès ainsi que les différents niveaux de classification.

7 https://tmm.dslab.ch/#/home




Cette fiche technique est une visualisation des informations jugées comme primordiales pour la représentation d'une entreprise. Elle représente les besoins exprimés par les parties prenantes sous une forme visuelle et permet de définir la forme d'un livrable potentiel pour TMM 2.0.


Ce graphique représente le score final attribué pour les outils testés en fonction de différents critères d'analyse. Ces critères font références aux besoins identifiés pour TMM 2.0 et sont basés sur des benchmarks utilisés dans le domaine de l'Intelligence Economique.

De plus, des maquettes d'interfaces et de fonctionnalités ont été ajoutées afin d'aider au développement de l'outil. Ci-dessus, on trouve un exemple d'une fiche technique d'entreprise qui pourrait être générée avec l'outil TMM 2.0.

Pour terminer, une série de recommandations managériales ont été formulées afin de supporter les décisions stratégiques. Ces dernières insistent sur le fait d'utiliser des méthodes agiles dans le développement de ce projet afin d'éviter une trop grande différence entre les résultats finaux et les besoins évolutifs des utilisateurs. En effet, ces derniers sont sujets à des variations en fonction de l'évolution des métiers et des technologies. Sur un projet d'une telle ampleur, il serait dangereux de fixer des exigences au début du processus et de ne pas pouvoir revenir sur celles-ci en cours de route.

D'autres recommandations au sujet de l'intégration des sources internes et du niveau d'analyse des informations ont été formulées afin d'aider à la prise de décision sur ces points essentiels pour le futur de l'outil TMM. Pour terminer, ce travail a été mené conjointement avec une thèse de bachelor réalisée à la Haute Ecole de Gestion de Genève par David Marques. Son travail avait pour but d'analyser différents outils choisis en fonction des besoins identifiés pour TMM 2.0. Cette analyse a permis de classer ces différentes plateformes afin d'aider à la prise de décision concernant l'intégration, ou non, de ces dernières.

## Conclusion

Premièrement, ce travail a permis de découvrir et cartographier l'écosystème mis en place par la Confédération pour lutter contre les cyberrisques. Les unités administratives impliquées dans la cyberdéfense sont connues, mais manquent parfois d'une vue d'ensemble et d'une coordination interdépartementale efficace. C'est pour pallier à ces problématiques que le nouveau centre national pour la cybersécurité (NCSC) a été mis en place. Il a pour but d'être le point central pour les questions liées à la cybersécurité ainsi que de mettre en œuvre et coordonner la SNPC.

On peut également remarquer une faiblesse structurelle dans cet écosystème due au système d'économie planifiée de l'administration fédérale. En effet, la plupart des unités doivent lutter entre elles pour avoir les ressources nécessaires pour produire de la cyberdéfense. Comme cela implique plusieurs départements, certaines querelles politiques s'ajoutent sur ce problème. De ce fait, un certain temps est investi dans des activités de *lobbying* pour obtenir plus de financement ou de ressources humaines et cela au détriment du travail effectif dédié à augmenter la sécurité de la Suisse. Bien entendu, ce n'est pas le cas partout mais ce genre de comportements économiques a pu être relevé plusieurs fois. Afin de pallier à ces problématiques, il est nécessaire de bien définir les missions et compétences de chaque entité dédiée au domaine cyber, mais également d'investir les moyens nécessaires pour la défense dans le domaine cyber, au même titre que dans les autres sphères d'opérations.

On peut aussi remarquer que la cyberdéfense est trop souvent perçue par son point de vue technique. Bien entendu, la sécurité informatique nécessite une forte composante technique, mais une approche holistique est nécessaire si l'on veut être efficace et efficient. Des domaines variés tels que le management, l'économie et les sciences sociales sont nécessaires pour développer une cyberdéfense complète. Cela permet par exemple d'optimiser la gestion des ressources, d'implémenter des politiques et des prescriptions légales et d'optimiser les partenariats entre les différents écosystèmes (publics, privés et académiques).

Finalement, une fois les futurs développements effectués pour TMM 2.0, on pourrait envisager d'automatiser la réalisation de cartographies ou de réaliser d'autres projets impliquant des analyses de données quantitatives relatives au domaine cyber. Cet outil devra à terme selon la SNPC, servir à toute l'administration fédérale comme référence concernant l'anticipation technologique.

K. C. & A. M.

Le Dr. Dimitri Percia David est bénéficiaire du premier Cyber-Defence Campus (CYD) *Distinguished Postdoctoral Fellowship* et chercheur postdoctoral à la Faculté d'Economie et de Management de l'Université de Genève, plus précisément à l'Information Science Institute. Son superviseur, le Dr. Thomas Maillart est maître d'enseignement et de recherche dans la même faculté et le même institut, et est spécialisé dans la recherche sur l'intelligence collective et les cyber-risques. Interview conjoint.

*Armasuisse S+T*

## Technometrics : La science au service de la veille technologique pour la cyber-défense

**Propos recueillis par le Dr. Alain Mermoud**
Rédacteur adjoint RMS+

**Comment fonctionne la collaboration entre l'Université de Genève et le *CYD Campus* d'armasuisse Sciences et Technologies (S+T) ?**

**Dimitri Percia David (DPD) :** *L'École polytechnique fédérale de Lausanne (EPFL) et le CYD Campus s'engagent conjointement en faveur de la recherche et de la formation dans le domaine de la cyber-défense. Les « Cyber-Defence Fellowships » sont ouverts aux chercheurs de niveau master, doctorat et postdoc. Deux postulations par année sont possibles, en principe au printemps et en automne. Une pré-sélection a lieu sur la base d'une proposition de recherche. Les candidats retenus se voient alors attribués, par un comité scientifique indépendant, un « Scientific Project Manager » du CYD Campus en fonction du sujet de recherche choisi.*[1] *Dans mon cas, c'est le Dr. Alain Mermoud, chef de la veille technologique au sein du CYD Campus, qui m'a été attribué. En parallèle, il est important de sélectionner un superviseur dans une haute école suisse qui a la volonté et la capacité d'encadrer une recherche scientifique liée à la cyber-défense. Dans mon cas, le choix du MER Dr Thomas Maillart s'est fait naturellement et rapidement, car son expertise conjointe en innovation, intelligence collective et modèles quantitatifs liés aux cyber-risques est incontestablement unique. Si vous étudiez au sein d'une haute école suisse et souhaitez faire progresser la recherche dans le domaine des sciences de la sécurité et des données, les « CYD fellowships » sont faits pour vous ! Plus d'information et inscription sur le site du CYD Campus : http://cydcampus.ch*

**Thomas Maillart (TM) :** *Du point de vue de l'Université de Genève, ce « fellowship » est considéré comme une entrée de fonds de recherche, comme dans le cas de l'obtention d'une bourse du Fonds national suisse de la recherche scientifique (FNS), par exemple. D'ailleurs, les « CYD fellows » sont rémunérés et engagés aux conditions du FNS. Dans le cas d'un postdoc, le financement est garanti pour deux ans. C'est évidemment un grand honneur pour l'Université de Genève d'avoir décroché le premier postdoc « CYD fellowship » ! L'initiative d'armasuisse S+T comble un vide important et permet l'émergence d'un « DARPA helvétique » (ndlr : l'agence pour les projets de recherche avancée de défense du département de la défense des Etats-Unis), au sein duquel des projets d'innovation hors du commun (« moonshot ») ont clairement le potentiel d'émerger et d'aider à développer des délivrables concrets pour le futur de la cyber-défense. Je me réjouis vivement de collaborer avec le CYD Campus et de contribuer au développement scientifique de la cyber-défense via le projet « Technology & Market Monitoring » (TMM 2.0), déjà évoqué dans la RMS+ N°3 2020.*[2]

**En quoi la veille technologique est une activité importante pour la cyber-sécurité ?**

**DPD :** *Comme le souligne la « Stratégie nationale pour la protection de la Suisse contre les cyber-risques » (SNPC, 2018-2022), la veille de marché et l'identification précoce des technologies émergentes et/ou de rupture constitue un élément clé de la stratégique de cyber-défense de notre pays. Parler de veille de marché et d'identification précoce, c'est parler de renseignement lié au développement technologique. Aussi, le développement d'une capacité de cyber-défense passe nécessairement par le renseignement sur les menaces, puisque ce n'est qu'au travers de ce dernier que l'on peut classifier les menaces par niveau de dangerosité et de probabilité d'occurrence – deux facteurs-clé de l'analyse du risque. Une analyse minutieuse, systématique et continue des innovations*

1 Les sujets de recherche d'intérêt pour le CYD Campus sont disponibles sur le site de l'EPFL : https://www.epfl.ch/research/services/fund-research/funding-opportunities/fellowship-mobility/cyd-fellowships/cyd-master-thesis-topics/ (consulté le 29.09.20)

2 Maillart, T. ; Mermoud, A. *L'intelligence collective et la veille technologique pour faire face aux défis de la cyber-défense, in* Revue Militaire Suisse (RMS+) N°3 - 2020.

*technologiques est ainsi nécessaire pour déceler leur impact en termes de risques (menaces potentielles) et opportunités (réponses appropriées). Une telle analyse demande ainsi une capacité de veille du marché technologique lié à la cyber-défense, mais également et surtout une capacité d'identification précoce des technologies impactant la cyber-défense.*

*De manière plus large, le développement d'une capacité de cyber-défense s'inscrit dans la politique et les procédures d'acquisition d'armement du DDPS, selon les recommandations du cabinet Deloitte rendues publiques en juin 2020.*[3] *La démarche de poursuite de la mise en place de capacités de cyber-défense s'inscrit dans la perspective des grands projets de ces quinze prochaines années, notamment le renouvellement des moyens de protection de l'espace aérien (Air2030), et la modernisation des Forces terrestres. Or, dans le contexte de développement d'une capacité de cyber-défense – impliquant du matériel d'armement à fort contenu informatique –, il existe un risque lié à l'obsolescence prématurée des systèmes. Ainsi, les systèmes risquent d'être déjà obsolètes au moment de leur introduction auprès de la troupe alors qu'ils ne l'étaient pas encore lors de la décision d'acquisition. L'intervalle entre le temps nécessaire à l'acquisition du matériel (temps d'acquisition) et la décroissance de l'efficience technologique (temps technologique) est un problème propre à l'acquisition de matériel informatique et au développement d'une capacité de cyber-défense. Une activité de veille technologique devrait alors permettre de réduire l'intervalle entre le temps d'acquisition et le temps technologique en sélectionnant les technologies les plus pertinentes à acquérir. En tant que commandant de compagnie, je suis particulièrement sensible à cet élément. Ainsi, la plateforme TMM sera également capable de suivre les développements technologiques relatifs au cyber-espace afin d'établir une image globale et en déduire des conséquences pour soutenir à la fois les développements stratégiques et la politique d'acquisition de matériel du DDPS, comme prévu dans le Plan d'Action Cyber-défense (PACD).*

**TM :** *Jamais la technologie n'a évolué aussi vite qu'aujourd'hui. Du jour au lendemain, des technologies émergentes font leur apparition, et certaines changent radicalement le contexte et l'environnement de la cyber-défense. De ce fait, il est critique de pouvoir anticiper les technologies qui vont faire la différence à court, moyen, et long terme. Il est important de bien modéliser les structures et dynamiques associées à une multitude de technologies en cours de développement, et ce afin de mieux pouvoir émettre des recommandations visant à adapter l'investissement et l'acquisition des technologies. Lors de la préparation de la première stratégie de cyber-défense de la Suisse en 2011, j'avais été invité à donner un séminaire dans lequel je recommandais à la Confédération d'investir – via un fond spécial de capital-risque labellisé cyber-défense – dans les technologies émergentes ayant un impact potentiel pour la cyber-défense. Le projet TMM 2.0 a clairement pour but d'opérationnaliser cette proposition formulée il y a maintenant presque 10 ans.*

**Vous évoquez la SNPC. Dans le cadre de cette stratégie, comment est-ce que votre recherche contribue au développement d'une capacité de veille technologique pour la Confédération ?**

**DPD :** *Afin de répondre à la mesure 1 (détection précoce des tendances ou technologies et acquisition des connaissances utiles) de la SNPC, le CYD Campus développe un « Tech Watch Program » avec sa propre plateforme de veille technologique inspirée de la base technologique et industrielle importante pour la sécurité (BTIS), qui constitue un élément important de la politique d'armement. La BTIS englobe les instituts de recherche et les entreprises installés en Suisse et disposant de compétences, connaissances et capacités en matière de sécurité et de défense. En 2018, la procédure d'auto-inscription dans la base de données BTIS a été remplacée par une « Surveillance des Technologies et des Marchés » (STM ; TMM en anglais) automatisée. Les données sont désormais récoltées via un robot d'indexation (web crawler) qui explore des sources publiques comme les registres du commerce, les sites web d'entreprises ou encore les réseaux sociaux. Les données sont recherchées à intervalles réguliers et mises à jour tous les mois dans la plateforme STM. La STM permet de retrouver des entreprises ainsi que les informations qui s'y rapportent, comme les produits, les services, les experts, et les technologies qu'elles proposent. Ces entreprises sont par conséquent visibles tant comme fournisseurs (ou sous-traitants) potentiels que comme partenaires de compensation éventuels dans le cadre d'une acquisition. En outre, nous effectuons des analyses sur mesure pour le compte du Secrétariat général du DDPS et le nouveau Centre national pour la cyber-sécurité (NCSC) qui est le centre de compétences de la Confédération en matière de cyber-sécurité et le premier interlocuteur pour les milieux économiques, l'administration, les établissements d'enseignement et la population pour toute question relative à la cyber-sécurité. Avec le NCSC, qu'il a placé sous la direction du délégué de la Confédération à la cyber-sécurité (ce dernier dépend directement du chef du Département fédéral des finances (DFF)), le Conseil fédéral entend renforcer le rôle actif de la Confédération dans la protection de la Suisse contre les cyber-risques. Notre objectif est donc d'alimenter la Confédération, via le CYD Campus, en produits (livrables) de veille technologique et pas uniquement le DDPS.*

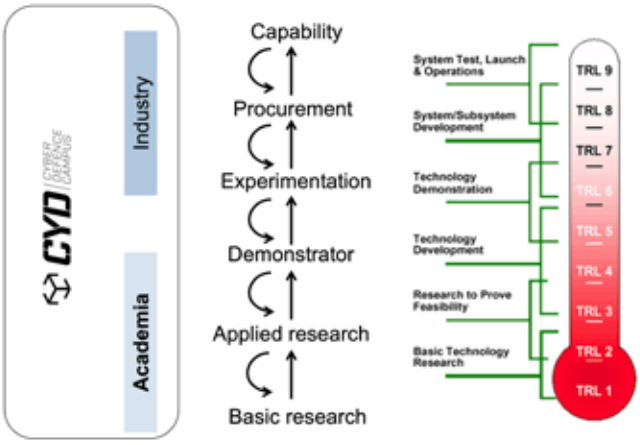
**TM :** *Du point de vue de la littérature scientifique, la veille technologique est une sous-discipline du « Technology Management ». Notre objectif est de contribuer à l'amélioration de la plateforme STM grâce à notre expertise scientifique. D'autre part, nous exploitons les données collectées à des fins scientifiques. Par ailleurs, cet outil a pour but d'automatiser de manière continue : 1. la* ***surveillance*** *des développements technologiques en général et le suivi de leur évolution/adoption au sein du marché ; 2. la* ***prédiction*** *des tendances*

3 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-79450.html (consulté le 29.09.20)

*et des développements technologiques, incluant l'anticipation des technologies de rupture (disruptive) ; 3. l'**évaluation des risques et des opportunités** des développements technologiques pour la cyber-défense. Ces trois buts permettent de : a. délivrer une identification précoce des tendances technologiques en distinguant et en cartographiant les acteurs (industrie : entreprises, fournisseurs, etc. ; recherche scientifique : chercheurs-clé, laboratoires, projets, etc.), les clusters technologiques et les hubs géographiques par cluster ; b. anticiper les tendances technologiques et évaluer les risques et les opportunités liés à ces mêmes tendances technologiques. Il sera alors possible d'identifier et de cartographier les organisations et les personnes associées à une technologie, d'établir des liens et d'éclairer les relations entre les différentes entités liées à une technologie donnée, d'identifier les changements de positionnement technologique des différentes entités liées à une technologie donnée, de délivrer une profilage des différentes communautés technologiques, de prédire les tendances technologiques et les futurs acteurs-clé , et d'observer le potentiel latent de synergies entre des disciplines scientifiques et des technologies.*

**De nombreux consultants – comme Gartner ou Forrester – offrent des services de veille technologique. En quoi votre approche est-elle différente ?**

**TM :** *Notre objectif est de fournir des modèles quantitatifs de prévision technologique et des outils de surveillance du marché pour la cyber-défense, basés sur les méthodes fournies par la science des données (data science). En partant d'une perspective socio-technique des systèmes d'information, nous appliquons certains principes de la physique appliquée à l'économie, de l'apprentissage machine (machine learning), et de la microéconomie au domaine de la cyber-défense. Une telle approche va permettre développer un tableau de bord quantitatif pour surveiller de quelle manière les technologies : (i) émergent, (ii) attirent une attention plus large (notamment en différenciant les bulles technologiques et le potentiel à long terme), (iii) se développent et mûrissent soudainement ou progressivement, et (iv) deviennent pertinentes en termes d'investissement, en particulier dans la perspective de la cyber-défense. Pour ce faire, nous procédons en plusieurs étapes : Premièrement, nous analysons les réseaux de capacité de production, les structures et les dynamiques de l'innovation qui sous-tendent le cycle de vie de chaque technologie, en particulier son niveau de maturité technologique (« Technology Readiness Level », TRL). Puis nous développons des modèles prédictifs, grâce à l'intelligence artificielle, pour évaluer le potentiel de croissance de chaque technologie, et ses conséquences prédictibles pour la cyber-défense. Enfin, nous modélisons des portefeuilles d'investissements par classes de technologies, afin de mieux diriger les investissements publics et privés, en particulier de manière à diversifier les risques extrêmes liés aux technologies émergentes.*




Infographique présentant le cycle de création d'une capacité de cyber-défense : Par le biais d'un écosystème tripartite d'experts en cyber-sécurité – mêlant l'industrie (entreprises et « hubs » technologiques), le monde académique (laboratoires et chercheurs de référence) et armasuisse S+T –, une importante émulation d'idées et de projets voit le jour. Les besoins en termes de biens et services liés à la cybersécurité deviennent alors l'objet de recherches fondamentales et/ou appliquées, menant ainsi à des « proofs-of-concept » qui, lorsqu'ils s'implémentent de manière satisfaisante, deviennent intéressant pour les programmes d'acquisition et d'achats de matériel, contribuant à la création d'une capacité de cyber-défense. A droite, le modèle de « Technology Readiness Level » (TRL) permet d'estimer le degré de maturité d'une technologie donnée, et peut donc être mis en parallèle avec le modèle de création de capacité en cyber-défense. Source : armasuisse S+T.

**DPD :** *La société Gartner propose une courbe de « maturité technologique » (parfois aussi appelée « hype curve »). Bien qu'elle semble intuitivement assez juste, cette courbe ne repose pas sur une analyse scientifique solide. Les techniques classiques de veille stratégique et d'identification précoce des tendances technologiques sont essentiellement basées sur des analyses qualitatives telles que : 1. des approches intuitives (jugement personnel, opinion d'expert, opinion de groupe d'experts, ou encore sur des méthodes structurées d'évaluation d'opinions de groupes d'experts, la méthode Delphi faisant référence dans ce domaine) ; 2. des approches mécanistiques comme la mise en réseau graphique, l'extrapolation de tendances ou encore des modèles de causalité ; 3. un mélange des deux premières méthodes. L'approche actuelle souffre de 2 problèmes : d'une part, elle n'est ni systématique ni quantitative et ne permet donc pas délivrer des prédictions solides. D'autre part, à l'heure de la multiplication d'inventions technologiques qui peuvent vraiment faire la différence (« game changer »), l'approche actuelle ne peut pas être appliquée à très large échelle. Les techniques de la science des données et de l'intelligence artificielle permettent de tester et valider un très grand nombre de scénarios au fur et à mesure que des données actualisées sont fournies à nos modèles.*

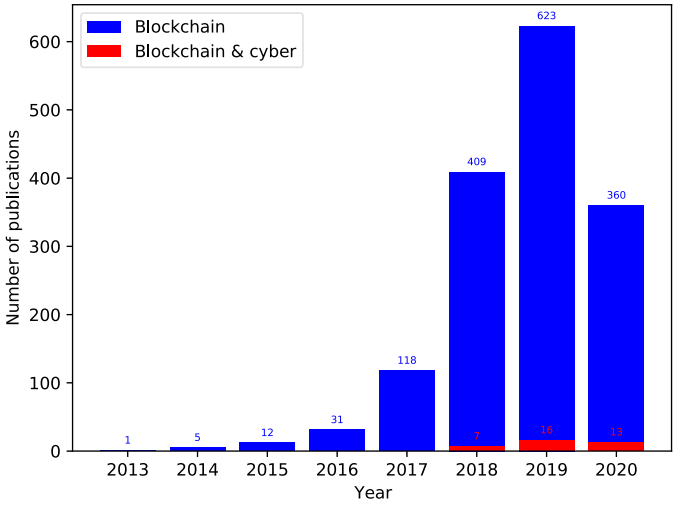
**Quels sont les technologies qui vont le plus influencer la cyber-défense à court, moyen et long terme ?**

**DPD :** *A court terme, on peut évidemment citer la technologie 5G. Pour rappel, en Suisse, deux groupes d'entreprises s'affrontent pour la 5G : d'un côté Sunrise et Huawei, de l'autre Swisscom et Ericsson. Les Etats-Unis affirment avoir trouvé la preuve que Huawei espionne pour le compte de la Chine. Ils font donc pression sur la Suisse, ainsi que sur l'Allemagne, pour qu'elles renoncent aux technologies chinoises pour le développement de la 5G. Pour l'instant, les autorités suisses voient le dossier Huawei davantage comme le théâtre d'une guerre commerciale que comme un problème de sécurité. Cependant, la polémique autour de ce dossier démontre que l'implémentation d'une nouvelle technologie échappe rarement à des logiques de guerre économique, mais aussi à des considérations géopolitiques.*

*Aussi, lors d'un séminaire stratégique de deux jours, les experts du CYD Campus ont identifié un portfolio de technologies pouvant avoir un impact sur la cyber-défense à moyen terme. Citons par exemple : les intelligences artificielle et collective (« artificial intelligence » (AI), et « swarm intelligence »), les senseurs et la sécurité de l'Internet des objets (« Internet of Things » (IoT) en anglais), le « edge computing », les mécanismes de préservation de la vie privée, l'apprentissage profond (« deep learning »), le E-ID, le « graph analyse », etc. Au cours des deux prochaines années, nous allons analyser chaque technologie identifiée une par une afin de déterminer son impact potentiel sur la cyber-défense. Concernant la prospective à long terme, armasuisse S+T poursuit, sous la conduite du Dr Quentin Ladetto, le programme de recherche en veille technologique DEFTECH[4] dont le but est de détecter les technologies à caractère disruptif ainsi que d'anticiper leurs impacts pour le monde militaire en général, et l'Armée suisse en particulier. Le CYD Campus poursuite également une activité de « scouting » à l'international (ndlr : évoquée dans ce numéro de la RMS). Cette activité nous permet d'injecter du renseignement technologique d'origine humaine dans notre recherche.*

**TM :** *A long terme, le calculateur quantique (« quantum computing » en anglais) aura d'une manière quasi certaine un impact très important sur la cyber-défense, en particulier sur la cryptographie, mais aussi sur la puissance de calcul. Cependant, il faut se méfier des modes. Le CYD Campus a récemment conduit une recherche sur les cas d'utilisation de la technologie Blockchain pour la cyber-défense. Les résultats montrent que cette technologie (très à la mode dans la fintech) semble n'apporter qu'un gain marginal dans le domaine spécifique de la cyber-défense. Nous espérons qu'une approche scientifique neutre permettra de rester en permanence concentré sur les innovations technologiques qui vont vraiment faire la différence.*

4 https://deftech.ch/ (consulté le 29.08.20)




Cet histogramme indique le nombre de publications sur arXiv.org (une archive ouverte de pré-publications électroniques d'articles scientifiques) contenant les mots clés « blockchain » (en bleu) et « blockchain AND cyber* » (en rouge) dans le titre et le résumé. A partir de 2018, un engouement (hype) clair est visible, alors que seul un petit nombre de publications liées à la (cyber-)sécurité et à la blockchain apparaissent. Cela montre également que les préoccupations de sécurité d'une technologie émergente arrivent souvent dans une deuxième phase. Source : chiffres fournis par Sébastien Gillard et Dimitri Percia David.

**Est-il possible de s'informer, de contribuer, ou de collaborer à vos recherches ?**

**TM :** *Outre sa rigueur d'exécution, une recherche scientifique de qualité doit nécessairement trouver sa source dans des problèmes concrets, si possible pour lesquels il existe des éléments empiriques (c'est-à-dire des données de qualité suffisante). De ce point de vue, il est absolument vital pour nous de dialoguer avec les organisations directement concernées par la cyber-défense, telles que les autorités publiques, les entreprises spécialisées et les infrastructures critiques, afin d'affiner nos questions de recherche. Pour cela, le 3 novembre 2020, nous aurons l'honneur de présenter les éléments-clé de notre stratégie de recherche lors d'une grande conférence au SwissTech Convention Centre de l'EPFL sur le sujet « Cyber-Threat & Technology Intelligence ». Il est aussi prévu que nous fassions un point d'avancement lors des « Swiss Cyber Security Days » (SCSD) qui auront lieu les 10 et 11 mars 2021 au Forum Fribourg. Enfin, nous organisons en septembre 2021, avec le Dr. Alain Mermoud et le Dr. Dimitri Percia David, la conférence internationale CRITIS (« International Conference on Critical Information Infrastructures Security ») à l'EPFL. Le sujet de cette année portera principalement sur le « technology forecasting, monitoring, foresight, and scouting » pour la protection des infrastructures et services critiques. Information et inscriptions sur : www.critis2021.org*

**DPD :** *Nous invitons tous les chercheurs intéressés à contribuer à nos recherches, à postuler pour un CYD fellowship. Par ailleurs, armasuisse peut, sous*


Le technology and market monitoring est une mission importante pour le CYD Campus.

*certaines conditions, établir un contrat de recherche avec un institut de recherche public ou privé. Pour les jeunes en formation, la Confédération offre également la possibilité d'effectuer un stage dans notre équipe de recherche ou d'exécuter une thèse de master (mémoire) au sein du CYD Campus. En cas d'intérêt, il convient d'envoyer une requête par e-mail (avec CV) directement à : cydcampus@armasuisse.ch. Par ailleurs, nous entretenons des contacts réguliers avec des scientifiques, lors de conférences internationales ou via des publications scientifiques de premier plan en physique, en économie, et en management. Grâce au réseau international du CYD Campus, nous avons des contacts réguliers avec nos homologues américains et israéliens qui se posent souvent les mêmes questions que nous. En France, nous suivons attentivement la recherche en Économie de Défense qui a récemment publié un document fondamental sur le rôle des technologies et de l'innovation dans l'autonomie et la défense d'un pays.*[5] *Au niveau de l'UE, nous collaborons avec l'Agence européenne de défense qui poursuit également un programme de Tech Watch*[6] *et le projet de recherche PYTHIA*[7] *(« Predictive methodologY for TecHnology Intelligence Analysis »). Au niveau Suisse, nous collaborons avec le laboratoire de systèmes d'informations répartis du Prof. Karl Aberer de l'EPFL, ainsi que l'Académie suisse des sciences techniques (SATW) qui publie chaque année un « Technology Outlook »*[8] *dans lequel des experts évaluent le potentiel de 37 technologies prometteuses pour la Suisse et son économie. En outre, je garde un fort lien avec mon ancien employeur, à la chaire Economie de Défense à l'Académie militaire (ACAMIL) à l'EPF de Zurich.*

*A. M.*

La 16ème édition de l'**International Conference on Critical Information Infrastructures Security (CRITIS 2021)** aura lieu du 27 au 29 septembre 2021 à l'EPFL SwissTech Convention Center. Cette conférence scientifique aura lien conjointement avec une conférence du CYD Campus réunissant des professionnels et des experts de la protection des infrastructures critiques.

Information et inscription: https://critis2021.org/

5 Mlizard, J. & Rademacher, B. (2020). Économie de défense: problématiques contemporaines. *Revue Défense Nationale*, 832(7), 7-11. https://www.cairn.info/revue-defense-nationale-2020-7-page-7.htm.

6 https://techwatch.eda.europa.eu/ (consulté le 29.08.20)

7 http://www.pythia-padr.eu/ (consulté le 20.08.20)

8 https://www.satw.ch/fr/cybersecurite/technology-outlook-2019 (consulté le 29.08.20)


Portion of Silicon Valley map by Maryanne Regal Hoburg (1982). Courtesy : The David Rumsey Map Center, Stanford University Library (CC BY-NC-SA 3.0)

*Armasuisse S+T*

## Exploration internationale des *start-ups* et de l'innovation pour le DDPS : Contribution du CYD Campus

**MSc EEIT ETH Giorgio Tresoldi**

Chef relations internationales Cyber-Defence Campus, armasuisse S+T

La Stratégie nationale pour la protection de la Suisse contre les cyber-risques 2018-2022 (NCS) souligne l'importance de la coopération internationale et de la coopération public-privé. Au sein du Département fédéral de la défense, de la protection de la population et des sports (DDPS), le Cyber-Defence Campus d'armasuisse Science et Technologies (S+T) sert de lien entre le monde industriel et le monde scientifique en matière de recherche, de développement et de formation à la cyberdéfense. Il est ainsi chargé d'identifier à temps les développements rapides dans le domaine de la cyberdéfense par le biais d'une surveillance technologique la veille internationale ainsi que de ses programmes de recherche.

### La technologie évolue rapidement : comment suivre le rythme ?

Aujourd'hui, la technologie et surtout le secteur des technologies de l'information progressent à un rythme de plus en plus rapide. A l'occasion de la publication du rapport Deloitte publié le 15 juin 2020, le DDPS souligne que : « *Il existe un risque, en particulier pour le matériel d'armement à fort contenu informatique, que les systèmes soient déjà obsolètes au moment de leur introduction auprès de la troupe.* »[1]

D'un autre côté, en raison du coût inférieur du matériel et de la disponibilité croissante d'une main-d'œuvre bon marché mais aussi grâce aux technologies les plus récentes (comme le cloud computing) la barrière d'entrée pour les entreprises dans le développement d'applications et de software n'a jamais été aussi basse. Ces conditions permettent aux entrepreneurs du monde entier de transformer des problèmes en opportunités pour lancer de nouveaux produits. Aujourd'hui, également dans le secteur de la défense, des produits brillants et innovants peuvent provenir de petites entreprises situées dans n'importe quelle partie du monde et pas nécessairement dans la grande industrie de la défense classique.

### Scouting internationl pour le DDPS

Cette évolution nécessite un changement dans la manière dont les gouvernements cherchent des solutions pour relever leurs défis en matière de TIC, de cybersécurité et de sciences des données. Il faut se mettre à l'œuvre sur le terrain, là où l'innovation se produit. Le CYD Campus tente de résoudre ces défis avec une combinaison d'analyses qualitatives et quantitatives : d'un côté par la plateforme de veille technologique et commerciale, qui prévoit de consolider toutes sortes de sources de données pour faire des observations et des prévisions sur les tendances actuelles. De l'autre avec une recherche plus approfondie sur des thèmes spécifiques qui est assurée par le programme (international) de veille technologique (Scouting) dont l'auteur de ces lignes est responsable.

Les objectifs de ce travail d'exploration sont d'analyser les technologies émergentes dans les domaines de la cybersécurité et de l'IA, de trouver des entreprises intéressantes sur la base des exigences du DDPS et de générer des projets de recherche conjoints et des preuves de concept avec ces entreprises.

Nous ciblons en particulier les entreprises émergentes mais aussi les entreprises bien établies si elles offrent des produits innovants. Afin d'accroître l'efficacité de nos efforts, nous sommes en train de mettre en place un réseau international de partenaires, qui peuvent nous aider à identifier les bonnes technologies. Il s'agit souvent d'investisseurs, de venture capitalists, d'incubateurs ou de structures locales et régionales de promotion des entreprises. La collaboration avec des autres gouvernements est également très fructueuse.

1 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-79450.html

### Certaines régions du monde connaissent une forte innovation

Nous avons également défini certaines limites géographiques afin de gérer la tâche et de nous concentrer sur la qualité plutôt que sur la quantité. Bien sûr, le plus grand *pool* d'entreprises se trouve aux Etats-Unis, la Silicon Valley et la baie de San Francisco vu les importantes sommes d'argent disponibles pour les *start-ups*. Les États-Unis sont également le plus grand marché et des régions à haute-innovation se développent à plusieurs endroits comme Boston, New York, Seattle, Austin mais aussi la région de Washington DC. Je reviendrais plus tard sur mon expérience personnelle aux Etats-Unis où j'ai été entre septembre 2019 et mars 2020.

Les autres régions que nous avons décidé de regarder de plus près dans un premier moment sont Israël, Royaume-Uni, la France, l'Allemagne et Singapour. Cette liste s'allongera inévitablement avec la poursuite et la consolidation de ce travail. Voici une brève motivation sur nos choix :

- Israël : La célèbre unité 8200 de l'armée israélienne constitue une excellente source de talents dans le domaine de la cybersécurité. De nombreux anciens soldats se dirigent vers l'industrie privée en fondant des startups ou en travaillant pour elles. Ceci, associé à la disponibilité des investisseurs, fait d'Israël un écosystème innovant. Toutefois, les défis politiques, éthiques et organisationnels qui pourraient découler de collaborations potentielles doivent être soigneusement pris en compte.
- Royaume-Uni : Londres abrite des universités re-nommées et le gouvernement dispose également d'un budget de défense considérable. La densité des entreprises dans le domaine des services financiers, contribue à l'essor des entreprises dans les domaines de la cybersécurité et de l'analyse des données.
- France : a commencé plus tôt à développer ses capaci-tés cybernétiques et peut désormais compter sur le Cyberpol de Rennes qui support la création de postes de travail qualifiés et soutient également les entreprises locales.
- L'Allemagne : Il est intéressant d'être un pays voisin et un partenaire économique important. L'Institut de cyberdéfense de l'Université de la Bundeswehr de Munich (CODE) et le Lernlabor Cybersicherheit de l'Institut Fraunhofer sont deux bons exemples d'institutions d'excellence dans ce domaine
- Singapour : porte d'entrée de l'Asie du Sud-Est, pays le plus développé de la région, plaque tournante mondiale pour les transports et les finances et ayant l'une des dépenses militaires par habitant les plus élevées, c'est un pays intéressant pour notre travail de scouting

Malheureusement, en raison de la situation actuelle de pandémie, tous les voyages internationaux ont été arrêtés après le mois de mars ; par la suite, pour le moment, je n'ai pu me rendre qu'aux Etats-Unis afin d'explorer ce marché et de mettre en place un réseau.

> Silicon Valley is not the birthplace of all tech-based start-ups, nor is it the source of all venture capital. Yet, over the past fifty years, the Valley's entrepreneurs have refined the art of company-building into a science. [2]

### L'écosystème de l'innovation Silicon Valley

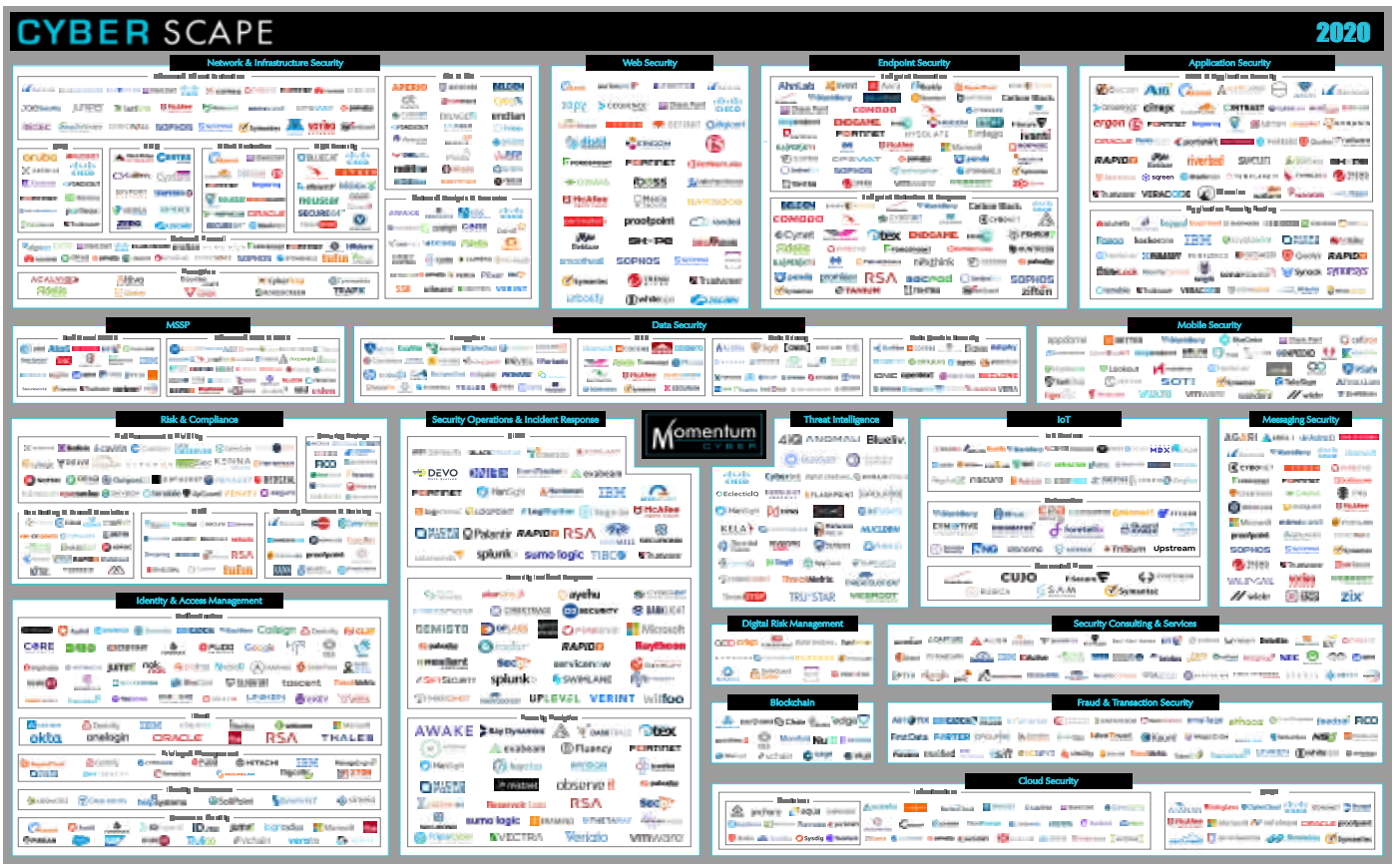
L'un des éléments nécessaires à l'innovation et à la création de nouvelles entreprises est l'argent, qui est l'un des atouts de la Silicon Valley avec ses écosystèmes de grands investisseurs. Il est important d'examiner les investissements car ils ont tendance à suivre les marchés qui sont dirigés par la demande des clients et peuvent donc indiquer des tendances. Cela se fait non seulement en consultant les données, disponibles gratuitement sur des plateformes en ligne telles que crunchbase, mais aussi en parlant directement aux entreprises d'investissement qui examinent leurs portefeuilles et obtiennent des informations sur les domaines qu'elles cherchent à développer.

Une autre partie très importante du travail aux Etats-Unis c'était l'échange étroits avec les avant-postes de Swisscom et Swissnex (un projet du Secrétariat d'État à la formation, à la recherche et à l'innovation SEFRI). Le Swisscom Cloud Lab Ltd. Est un centre d'innovation de classe mondiale qui, au fil des ans (fondé en 1998), a construit un important réseau stratégique aux États-Unis et au-delà. Il soutient Swisscom et ses clients en Suisse dans l'identification et le développement de nouvelles solutions afin d'apporter l'innovation sur le marché suisse. L'un des thèmes principaux du Lab est la cybersécurité, avec une équipe dédiée chargée de l'innovation et de la recherche de nouvelles entreprises et d'opportunités commerciales. Il compte aujourd'hui une dizaine d'employés qui analysent en permanence l'environnement et recherchent des *start-up* intéressantes pour le marché suisse. Une collaboration intensive a eu lieu au cours du séjour, qui a produit des résultats très fructueux au point que nous avons maintenant établi un partenariat pour continuer à partager des informations sur les tendances mondiales en matière de cybersécurité et d'analyse des données.

### Les accélérateurs et les investisseurs sont les catalyseurs de l'innovation

Un autre point très important pour mon travail était les Accélérateurs et les Incubateurs : Ces lieux aident les nouvelles entreprises à développer leurs produits et leur concept commercial en les mettant en contact avec des investisseurs et des clients potentiels, et en leur fournissant les outils et les connaissances nécessaires pour réussir.

Au cours des six mois passés aux Etats-Unis, j'ai rencontré plus de dix « multiplicateurs » tels que des investisseurs, des accélérateurs, etc. qui, combinés à mes propres recherches, m'ont permis de rencontrer plus de 70 entreprises. La quantité importante de matériel recueilli a donné naissance à plusieurs produits pour le campus de cyberdéfense et pour le DDPS. Mais le résultat le plus utile sont les preuves de concepts : Grâce à un échange régulier avec nos partenaires au sein de l'armée et de la Base d'aide au commandement (BAC), nous avons pu leur présenter de nouvelles technologies qui ont suscité leur intérêt. À partir de là, nous avons (et nous continuons) à mettre en place plusieurs « tests » de technologie dont le but n'est pas de comparer des entreprises, mais plutôt de se faire




Panorama des acteurs utiles pour les activités de scouting du CYD Campus.

une idée plus précise de l'état actuel de la technique, d'acquérir de l'expérience avec une technologie et de comprendre son fonctionnement. Cela pourrait aussi être utile pour mieux définir les exigences qui pourraient être nécessaires dans un processus d'acquisition futur.

À l'avenir, ce travail de recherche pourrait aider à réaliser certaines des suggestions formulées dans le rapport de Deloitte, comme la recommandation 3.28 pour « *cherche[r] des solutions novatrices à une problématique spécifique. Cela permet de combler de manière optimale des lacunes de capacités reconnues, mais aussi d'identifier dès que possible de telles lacunes.* » [3]

Du côté du contenu, l'espace de la cybersécurité est vaste et il existe une multitude de solutions logicielles et matérielles pour résoudre toutes sortes de problèmes. L'une des tendances est une certaine segmentation du paysage avec quelques grands fournisseurs qui couvrent de vastes zones de marché et des *start-ups* et des entreprises plus petites qui s'occupent généralement d'un problème précis. Par conséquent, l'intégration des différentes solutions dans l'écosystème existant devient d'une importance vitale. D'autre part, il n'est pas toujours facile de comprendre de quelle technologie s'occupe une entreprise. Une bonne cartographie de l'espace est réalisée par Momentum Cyber [4]. Cependant, cet exemple n'est qu'une petite pièce du puzzle et il ne suffit pas d'avoir de bonnes sources pour obtenir un bon résultat. Un élément clé reste l'interprétation et le filtrage des données afin de fournir aux destinataires des informations pertinentes.

En conclusion, sur la base des expériences acquise jusqu'à présent, nous poursuivrons et améliorerons ce travail à l'échelle mondiale. Le fait de disposer d'un bon réseau capable de fournir des pistes adéquates et intéressantes est la clé du succès. Heureusement, les entités suisses sont présentes dans le monde entier et peuvent généralement compter sur des réseaux locaux remarquables dans les pays respectifs. Certains des partenaires tels que Swissnex et Swisscom ont déjà été cités, mais d'autres comme l'organisation suisse de promotion des exportations et des investissements Swiss Global Enterprise, les attachés de défense ainsi que les responsables de la science et de la technologie (en tant que partenaires clés dans les ambassades) sont autant important. En plus de cela nous avons déjà identifié plusieurs partenaires dans le secteur public ainsi que privé dans toutes les nations susmentionnées avec lesquels nous travaillons déjà ou avec lesquels nous commencerons bientôt une collaboration afin d'établir un processus systématique de recherche, de sélection des technologies et d'innovation pour permettre au DDPS de se tenir au courant des derniers développements technologiques.

G. T.

**Références :**

[1]https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-79450.html
[2] Messina, Michelle E.. Decoding Silicon Valley: The Insider's Guide . Decode Publishers, LLC.
[3]https://www.newsd.admin.ch/newsd/message/attachments/61731.pdf
[4] https://momentumcyber.com/intel/

Responsable du programme de recherche « Prospective technologique » d'armasuisse S+T, Quentin Ladetto a récemment présenté, aux côtés de ses partenaires, le jeu de société « New Techno War ».

*Armasuisse S+T*

## Prospective technologique et simulation : Jouer aujourd'hui c'est gagner demain !

**Dr. Quentin Ladetto, Dr. Michael Rüegsegger**
armasuisse Sciences + Technologies (S+T)

Que vous attendiez des études et des rapports comme livrables d'un programme de prospective semble être une attente raisonnable. Arrêtons-nous cependant un instant et demandons-nous : sommes-nous vraiment intéressés par les technologies elles-mêmes ou par ce qu'elles offriront ; comment celles-ci affecteront notre mode de fonctionnement et quelles opportunités et menaces elles pourraient représenter ? À ce stade, allons même un peu plus loin et demandons-nous si ce qui nous intéresse vraiment, ce sont les opportunités, les menaces et ce qu'elles représentent ou si c'est ce qu'elles représentent pour nous ? Cette différence n'est pas anecdotique car elle signifie que nous devons passer d'un produit descriptif à quelque chose qui nous touche individuellement. La meilleure façon d'y parvenir est de générer une expérience unique, qui interagit avec nos sens, de sorte que nous puissions nous y référer en cas de besoin.

Travailler sur le récit, y compris en racontant des histoires, pourrait donc être une façon de faire vivre une expérience au lecteur. Malheureusement, l'expérience se trouverait réduite au niveau émotionnel. Permettre aux gens de jouer avec ce que la technologie permettrait et de vivre les conséquences de leurs décisions dans un scénario donné leurs apporterait certainement plus d'informations.

Il y a cependant un défi supplémentaire à relever : les éléments que nous voudrions expérimenter n'existent pas encore. Par conséquent, au lieu de les tester simplement, nous devrons les simuler. Se tourner vers le monde de la simulation avec des idées et des sentiments plutôt que des valeurs pour alimenter les modèles mathématiques n'est pas si évident. C'est à ce moment que le « jeu » est venu à l'esprit. Mais comment ? Avec quoi ? Avec qui ? À quel niveau ? Combien de temps ? Sans le savoir vraiment, nous avons ouvert la boîte de Pandore des possibilités et des alternatives que nous devrons envisager pour construire notre environnement ludique, notre écosystème technologique.

Ce que vous lisez ici est une tentative originale de présenter non seulement le travail accompli, mais également la motivation des différents acteurs impliqués dans ce voyage.

Ce projet s'inscrit dans le cadre du programme de recherche en prospective technologique d'armasuisse Science et Technologie, également connu sous le nom de Deftech (DEfence Future TECHnologies) et dont le but est d'identifier les tendances technologiques de rupture, d'évaluer leurs implications dans un contexte militaire et d'informer l'armée suisse des opportunités et menaces possibles.

### A la recherche du bon format

Compte tenu de l'expérience acquise lors de l'organisation et la participation à différents jeux de guerre, force est de constater que l'accent est mis sur la stratégie et non sur la compréhension des effets occasionnés par une nouvelle technologie ou une nouvelle arme.

Nous sommes arrivés à la conclusion, certes évidente a *posteriori*, que pour comprendre l'impact d'un nouveau produit, rendu possible par l'intégration de nouvelles technologies, nous devons le simuler au niveau où il est utilisé. Dans notre cas, il s'agit de passer du niveau stratégique au niveau tactique. Il nous faut donc définir pour ces futurs systèmes les valeurs de paramètres tels que la protection, la létalité, la mobilité. Comme l'accent est mis sur la compréhension des implications de l'utilisation du système, nous devons avoir la flexibilité nécessaire de modifier facilement les valeurs le définissant afin de comprendre quelle combinaison occasionnerait une révolution plutôt qu'un simple avantage tactique.

*Prenons l'exemple de l'exosquelette. Une des possibilités serait d'équiper certains fantassins pour qu'ils puissent se déplacer plus rapidement, porter plus de poids (protection ? munitions ?), être moins sujets à la fatigue*

Le jeu de guerre sous la forme de jeu de plateau facilite une discussion et un échange autour des futures technologies intégrées dans des futurs systèmes ayant un impact potentiel sur la tactique et la stratégie militaire. Ce jeu sérieux permet au joueur d'expérimenter les impacts de ces nouvelles possibilités bien avant que celles-ci ne soient réalisables.

*physique et aux blessures, etc. La grande question pour chacun de ces paramètres est de savoir «combien». Permettre au soldat de porter 80 kg au lieu de 50 kg peut être un avantage car cela pourrait signifier plus de protection ou plus de munitions compte tenu des circonstances, mais cette différence de 30 kilos justifie-t-elle à elle seule l'ampleur des développements requis? Et si au lieu de 80 kg, on pouvait transporter 800 kg?*

Le jeu doit donc permettre de simuler facilement ces changements et de stimuler les discussions qui les entourent. Le but n'est pas ici de gagner, mais de comprendre les forces et les faiblesses induites par ces futurs systèmes dans des scénarios tactiques donnés. L'option du jeu de plateau (Figure 1) fut donc retenue et le cahier des charges intègre les objectifs suivants:

- Le jeu sera créé autour de scénarios « bleu contre rouge ».
- Les règles doivent être suffisamment simples pour que les débutants puissent commencer à jouer en 15 minutes.
- La durée d'une partie doit être de 60 minutes au maximum afin de permettre le test de différentes options pendant une demi-journée.
- Le jeu doit être suffisamment modulaire pour permettre l'introduction de nouvelles technologies / systèmes futurs ainsi que de nouveaux scénarios afin de s'adapter aux intérêts et à l'orientation des différentes parties prenantes.

Partie prenante des développement, l'Etat-Major de l'armée suisse fut impliqué dans la définition des scénarios ainsi que dans la priorisation des technologies à considérer. Ensemble, nous avons veillé à ce que tout ce que nous simulons du côté bleu respecte les conventions de Genève. Nous avons validé les différents paramètres technologiques avec des experts afin de nous assurer que les valeurs initiales correspondent à des développements plausibles pour les années à venir.

C'est ainsi que nous avons entamé le voyage vers ce qui deviendra la plate-forme « New Techno War » (NTW) !

## Le défi de la simplicité

La majorité des jeux de guerre de plateau, dont les plus réussis commercialement, visent un réalisme total. On y parvient grâce à une mécanique de jeu précise et à des détails exagérés, au détriment de la simplicité. Il est rare de voir un manuel de règles de moins de 30 ou 40 pages minimum. Pour ce développement, nous avons dû inverser le paradigme afin de *simuler le plus précisément possible mais de rester aussi simple que possible*. Le résultat est le jeu New Techno War (Figure 2), dont le manuel de règles ne fait que 4 pages.

Nous sommes donc partis du principe qu'il fallait développer un jeu reprenant la doctrine suisse actuelle


Représentation du jeu de table « New Techno War » avec l'accent mis sur les nouvelles technologies et les nouveaux systèmes. Le titre « Challenge today tactics with the systems of tomorrow - Défie les tactiques d'aujourd'hui avec les systèmes de demain » résume ce que nous avons essayé de mettre en avant en jouant à ce serious game. Le jeu est disponible en français, allemand et anglais.

de manière simple et flexible. Flexible, parce que nous devons être capables d'affiner les paramètres du jeu pour voir clairement l'effet d'une nouvelle technologie qui a un impact sur ces paramètres et sur ces paramètres seulement.

*Prenons un exemple concret :* le renseignement. *Nous avons décidé que le renseignement devait être absolument présent dans le jeu, car il est un élément essentiel de la guerre moderne. Le renseignement est traité différemment selon que vous soyez l'attaquant ou le défenseur. En tant qu'attaquant, le principe de base est que vous disposez d'un renseignement initial presque complet sur les positions, les forces, les armes et la structure du défenseur ; mais au fur et à mesure que la bataille progresse dans le temps, l'incertitude augmente : l'arrivée des réserves, l'approvisionnement en munitions, le mouvement des troupes : tous ces éléments évoluent.*

*En tant que défenseur (pour rappel, la mission de l'armée suisse est uniquement défensive) votre qualité de renseignement au début de la bataille est presque inexistante car c'est l'attaquant qui choisit où et quand intervenir. Cependant, plus la bataille progresse, plus vous obtenez de renseignements, ne serait-ce que parce que vous prenez désormais part au combat.*

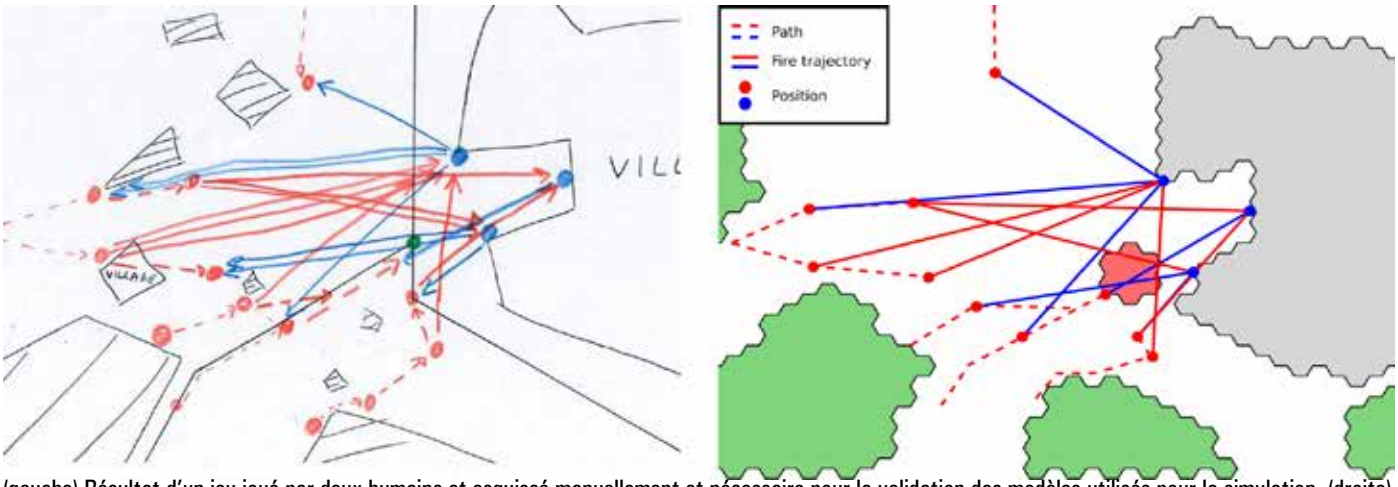
*Comment simuler cela ? L'attaquant commence avec un 6 en intelligence et perd 1 point par tour jusqu'à ce qu'il atteigne 4. Le défenseur opposé commence à 0 et voit sa caractéristique augmenter de 1 à chaque tour, jusqu'à ce qu'il atteigne 4. Ce point d'équilibre, trouvé au 4e tour du jeu, oblige l'attaquant à aller vite, alors que le défenseur a tout intérêt à ralentir l'attaque. Cela semble réaliste. Cette règle est expliquée en une ligne. Simplicité.*

*Ajoutons une nouvelle technologie principalement axée sur le renseignement : un essaim de drones. Le drone affecte la recherche de renseignements dans la zone qu'il survole et distribue ces renseignements à une personne ou à une troupe. L'utilisation d'un essaim de drones va donc se refléter sur 3 paramètres du jeu, à savoir : l'utilisation de drones va modifier la qualité du renseignement ; l'amélioration du renseignement est limitée à une zone spécifique ; une troupe ou une partie de celle-ci dispose de ce renseignement supplémentaire.*

*Pour les règles du jeu, cela se traduit par deux lignes spécifiques au système de l'essaim de drones. Simplicité.*

À ce stade, nous espérons que tous les acteurs autour de la table se rendent compte de l'apport d'un nouveau système dans une situation tactique spécifique bien mieux qu'en lisant un rapport à ce sujet. Il reste cependant une question ouverte que nous n'avons pas vraiment abordée : étant le défenseur ou l'attaquant, existe-t-il une façon spécifique d'utiliser ce nouveau système pour remplir ma mission ?

Répondre à cette question nécessite d'envisager toutes les possibilités d'utilisation du nouveau système dans ce scénario donné. Devant le nombre de parties à considérer, le passage du monde physique au monde numérique s'impose.




(gauche) Résultat d'un jeu joué par deux humains et esquissé manuellement et nécessaire pour la validation des modèles utilisés pour la simulation. (droite) Le même résultat dans sa version digitale.

## Du plateau à l'écran

Le passage au monde numérique présente quelques défis intrinsèques mais permet d'obtenir des informations supplémentaires sur la manière dont les nouveaux systèmes pourraient être utilisés et potentiellement remettre en question les procédures tactiques actuelles. Les efforts entrepris visent à améliorer la compréhension des questions suivantes :

- Que pouvons-nous apprendre en générant tous les résultats possibles d'un scénario ?
- Que peut apprendre un humain en jouant contre une Intelligence Artificielle (IA) ? Comment pouvons-nous le faire ?
- Quel type d'information pouvons-nous présenter au joueur humain pour que le tandem humain + IA soit meilleur que l'IA seule ? Comment présenter l'information au joueur ?

## Simulation de tous les résultats possibles

Le nombre de résultats plausibles dans tout jeu de guerre non trivial est si grand qu'il n'est pas possible pour un humain de les analyser tous. Cette incapacité à explorer tout un espace de résultats peut avoir une importance moindre si le jeu est utilisé pour l'entraînement et l'apprentissage, mais elle est d'une importance capitale si vous l'utilisez pour développer une nouvelle doctrine, pour tester des concepts d'opération et pour évaluer des décisions tactiques. Dans ce cas, vous devez faire la différence entre ce qui est possible, plausible ou probable.

Comment relever ce défi ? Grâce à ce qu'on appelle les simulations multi-agents. Comme les ordinateurs jouent plus vite que les humains, les simulations multi-agents peuvent explorer systématiquement tout l'espace des possibles d'un jeu et identifier les lignes de conduite optimales.

## Simulations multi-agents

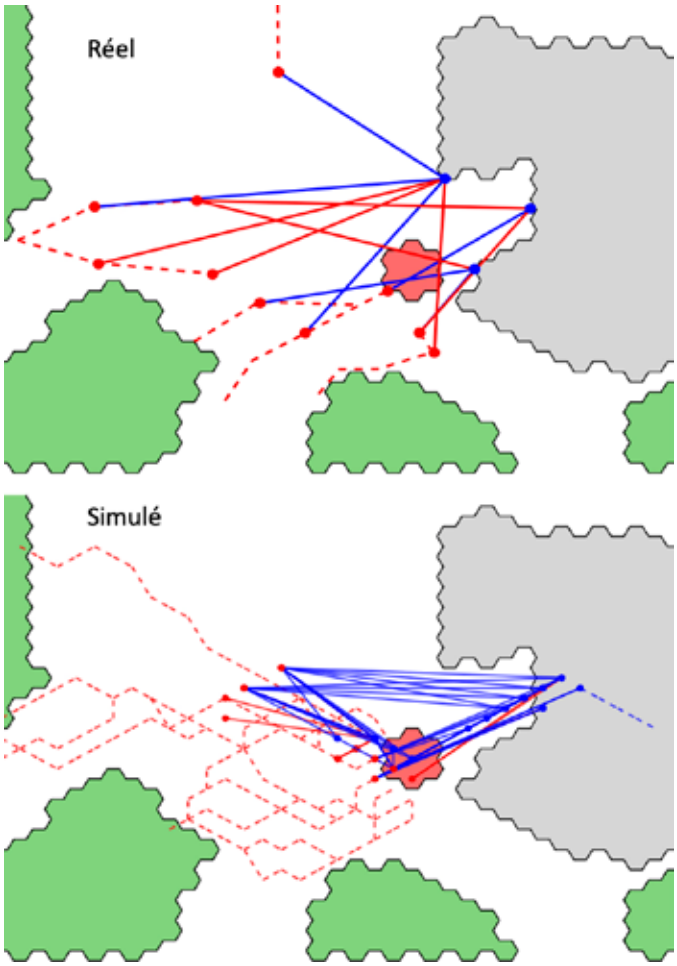
Les systèmes basés sur des règles, comme les jeux de plateau, peuvent être directement traduits en simulations : les règles du jeu et les environnements de jeu, comme le terrain et le temps, sont codés sous forme de modèles informatiques, qui avancent pas à pas, tandis que les résultats des interactions des joueurs sont enregistrés comme le nouvel état du monde simulé. En bref, c'est l'essence même des simulations multi-agents.

Les simulations multi-agents sont des *jumeaux numériques* du monde réel qui permettent de prendre en compte toutes les dynamiques et interactions que l'on trouve dans la vie réelle. Elles permettent de simuler aussi bien des villes, le commerce et les échanges financiers que des matches de football ou des opérations militaires. Pour construire une simulation multi-agents, une population synthétique est d'abord générée. Il s'agit d'un instantané statique du système d'intérêt, comprenant les propriétés sociodémographiques et les comportements des individus ainsi que l'environnement sociotechnique. La population synthétique est ensuite animée en fonction des règles de comportement et des contraintes environnementales à l'aide des technologies de simulation. La simulation est ensuite calibrée pour produire des résultats statistiquement indissociables des variables d'intérêt du monde réel. Ce type de simulation validée est non seulement utile pour explorer l'espace des résultats des jeux, mais aussi pour des diagnostics et des scenarios prospectifs.

## Simulation du jeu de guerre

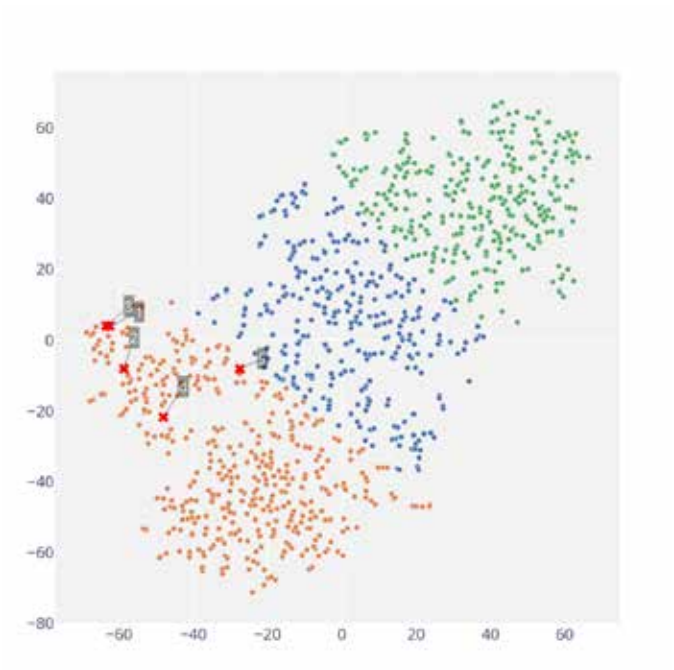
L'élaboration et l'exécution de la simulation multi-agents de NTW a comporté les étapes suivantes :

- **Familiarisation avec NTW** : plusieurs sessions de NTW ont été joués pour apprendre le jeu et comprendre les règles.
- **Construire le modèle NTW**, y compris les joueurs, l'équipement, la topographie et en y intégrant les règles du jeu.




Représentation digitale d'une partie jouée par deux adversaires humains. (pas) Simulation obtenue représentant la même situation. Il est important de vérifier que dans la multitude de simulations générées par les agents, on retrouve les parties jouées par les humains.

- **Encodage du modèle en tant que simulation multi-agents** : écriture d'un logiciel pour se rapprocher pour chaque scénario de la «physique» du jeu, comme une version numérisée du plateau de jeu ; description des forces en présence composées de systèmes, d'effecteurs et de plates-formes pour chaque scénario ; définition des objectifs de mission pour les agents, et équipement des agents avec des comportements d'apprentissage de renforcement.
- **Vérification et validation de la simulation :** les résultats des parties jouées manuellement ont été esquissés à la main (Figue 3, partie gauche). Les lignes pointillées bleues et rouges représentent la façon dont les unités militaires BLEUES et ROUGES ont été déplacées par les joueurs humains pendant le jeu. Les points bleus et rouges indiquent les positions de tir. Les lignes pleines bleues et rouges représentent les lignes de tir. Des croquis dessinés à la main ont ensuite été numérisés (Figure 3, partie droite) ; 1 000 simulations ont été effectuées et les résultats ont été automatiquement esquissés dans un format similaire aux croquis manuels (Figure 4). Enfin, les résultats des jeux manuels ont été comparés aux résultats des jeux simulés par des algorithmes d'apprentissage automatique développés pour la reconnaissance d'images.




Représentation de 1'000 résultats de parties simulées et représentées par un nuage de points. Les parties sont regroupées en trois groupes distincts. Les parties jouées par des humains, représentés par des croix rouges à gauche du nuage de points, ne ressemblent qu'au groupe de parties en brun. Les parties représentées dans les groupes bleu et vert sont des parties jouées par les agents digitaux. On constate que ces approches n'ont pas été considérées par les humains. La distance entre les points représente la différence entre deux ~~représentations~~ digitales de parties telles que présentées à la Figure 4.

- **Création d'un dispositif permettant de mener des expériences pour explorer l'espace des résultats du jeu et identifier les tactiques optimales.** Cela inclut la production de 10'000 simulations.

### Analyse des résultats

Comme indiqué au début, les simulations peuvent explorer tout l'espace des résultats plausibles du jeu. Nous n'avions pas l'intention de reproduire des résultats de jeu spécifiques, mais de savoir si l'intelligence artificielle qui alimente la simulation multi-agents possède les propriétés nécessaires pour produire des résultats plausibles qui transcendent l'imagination et le jeu humains. Tout d'abord, nous constatons que la simulation produit effectivement des résultats comparables à ceux des jeux auxquels les humains ont participé. Les jeux joués par les humains sont représentés par des croix rouges dans le groupe marron de la Figure 5. Le nuage de points représente 1 000 jeux simulés. Ensuite, trois groupes distincts se dégagent du regroupement des résultats des jeux par apprentissage machine. La signification de ce graphique devient alors évidente : *La simulation joue des parties et produit des résultats que les humains n'avaient pas imaginés.*

### Que révèlent les simulations ?

Les parties jouées par les humains suggèrent que BLEU peut gagner le NTW 40 % des fois. La simulation suggère

au contraire que BLEU a beaucoup moins de chances de gagner, environ 3 %. Considérant le nombre de nouvelles possibilités fournies par l'intelligence artificielle, cela apparait comme intuitivement correct. Après avoir ajusté les paramètres d'apprentissage de BLEU, le ratio de victoires de BLEU n'a pas dépassé 10 %. La simulation indique donc que les humains sont probablement trop confiants quant à leur possibilité pour BLEU de gagner. Cela peut s'expliquer par le fait qu'au départ ils n'étaient pas conscients des autres possibilités à disposition. Les humains s'enferment dans des schémas étroits et familiers ; ce qui n'est pas le cas des simulations. Les simulations aident donc à identifier des tactiques optimales sans être la proie à des biais cognitifs.

Éliminer les biais cognitifs en jouant contre un champion numérique, telle est l'ambition poursuivie dans le développement de deux intelligences artificielles (l'une jouant ROUGE, l'autre BLEU) pour NTW.

**Quand l'artificiel vient renforcer le réel.**

Les agents modernes basés sur l'intelligence artificielle (IA) surpassent les humains non seulement en termes de capacité à fournir des informations, mais aussi à prendre des décisions dans des situations contrôlées. Dans un monde miniature avec des règles et des actions données, un système informatique ne fournit pas seulement le contexte pour la prise de décision, mais est capable de décider par lui-même. Si une tâche de décision peut être lancée dans un monde aussi simplifié (généralement sous forme de jeu), alors très souvent une IA sur mesure peut aider à choisir les bonnes actions. La configuration décrite comprend pratiquement tous les jeux stratégiques, tels que les échecs, le go, le shogi, le hexagone, ... pour lesquels les IA battent sans effort les champions du monde humains.

Au cœur de cette percée technologique se trouve l'idée d'entraîner les IA en leurs faisant jouer des milliards de simulations. Chaque victoire ou perte est enregistrée et l'IA est améliorée à chaque étape. Non seulement une simulation est fournie au décideur, mais l'IA passe en revue autant de cas raisonnables que possible et sélectionne les actions qui ont le plus de chances de donner les meilleurs résultats. Après un nombre suffisant d'itérations, cette procédure donne lieu à des mouvements inédits qui dépassent les capacités des maîtres humains dans pratiquement tous les jeux stratégiques.

**Une IA tactique**

Le jeu NTW sert de modèle simplifié mais réaliste pour la prise de décision dans divers scénarios de situations réelles. Le joueur est confronté à une situation typique de conflit militaire et doit décider de la stratégie et de la tactique à adopter pour atteindre ses objectifs militaires. Bien entendu, le joueur peut se livrer à un nombre limité de scénarios, ou simulations, dans son imagination et prendre les meilleures mesures sur la base de l'expérience, des données disponibles et de la simulation. Cependant, des méthodes d'entraînement des agents de l'IA ont été établies pour de nombreux autres jeux afin d'atteindre des performances surhumaines. Une approche basée sur l'IA est mise en œuvre pour NTW dans le but d'apprendre les tactiques et stratégies militaires. Une fois qu'il atteint des performances satisfaisantes dans le cadre des règles du jeu, la structure du jeu peut être étendue pour saisir plus précisément la réalité de la guerre. Les exemples incluent l'ajout de futures armes et la spécification plus détaillée de leurs propriétés, l'incorporation d'agents supplémentaires avec des objectifs distincts, etc.

**IA pour les jeux stratégiques**

En ce qui concerne le développement des joueurs d'IA pour les jeux stratégiques (y compris les échecs, le go, le shogi, l'hexagone,...), deux méthodes de recherche des meilleures décisions peuvent être considérées comme standard. Nous décrivons ces approches en détail ci-dessous.

Tout d'abord, il y a la recherche classique dans laquelle un joueur d'IA tente de simuler le plus grand nombre possible d'états de jeu et choisit ensuite la meilleure des simulations. Cette approche peut être décrite comme de la force brute en ce sens que son but ultime est d'essayer tous les états de jeu possibles et de suivre les décisions qui mènent à la victoire. En pratique, une recherche exhaustive n'est généralement pas possible car même les jeux simples dépassent rapidement la capacité des ordinateurs les plus puissants. Le nombre d'états de jeu raisonnables aux échecs est estimé à environ $10^{40}$, un nombre bien au-delà de la portée de la simulation informatique. En conséquence, tous les états ne sont pas analysés, mais l'IA se limite à un nombre suffisant de résultats raisonnables. La recherche est quantifiée par deux paramètres clés.

Le *facteur de ramification* mesure le nombre d'actions raisonnables que le joueur adverse peut prendre, compte tenu de la décision en cours. La *profondeur de recherche* définit le nombre d'actions conséquentes simulées. Aux échecs, le facteur d'embranchement typique est d'environ 3, c'est-à-dire que pour chaque coup, 3 réponses sont généralement prises en compte, et une profondeur de 80 coups au maximum. Une fois que la largeur (donnée par le facteur d'embranchement) et la profondeur de recherche maximales sont atteintes, une évaluation personnalisée mesure la qualité du résultat. Un algorithme d'IA commun qui met en œuvre cette approche est la recherche dite AlphaBeta. Il convient de mentionner que les programmes d'échecs publics qui mettent en œuvre l'algorithme AlphaBeta (comme par exemple StockFish) et qui fonctionnent sur un smartphone disponible dans le commerce jouent beaucoup plus fort que le champion du monde d'échecs humain.

Si AlphaBeta est extrêmement efficace dans une situation où le facteur de ramification et la profondeur de recherche ne sont pas trop importants, il échoue rapidement lorsque ces paramètres augmentent. En raison de la nature exponentielle de l'exercice de recherche, même une unité de profondeur supplémentaire multiplie la capacité

Interface Web du jeu numérisé New Techno War permettant aux joueurs humains de défier les Intelligences ~~Arifitives~~ entraînées spécifiquement pour ce jeu.

requise de l'ordinateur par le facteur de ramification. Par conséquent, ce problème ne peut être résolu en se contentant de choisir de meilleures infrastructures de calcul.

La seconde méthode, plus moderne, de prise de décision dans les jeux, traite explicitement des faiblesses de la recherche AlphaBeta et peut être décrite comme une recherche dirigée. Diverses architectures ont été proposées, mais la configuration de base est la suivante. Deux réseaux neuronaux profonds (Deep Neuronal Network - DNN) sont utilisés pour la prise de décision. Le premier est évaluatif dans le sens où il mesure la qualité des positions. Le second DNN dirige la recherche en estimant les probabilités d'actions raisonnables. Par rapport à AlphaBeta, cette méthode se concentre davantage sur les conséquences probables et pertinentes d'une décision plutôt que de vérifier le plus grand nombre possible. Les algorithmes de recherche de ce type sont résumés sous l'acronyme MCTS (Monte Carlo Tree Search). Ces dernières années, les algorithmes de recherche MCTS ont surpassé la recherche AlphaBeta pour de nombreux jeux, notamment les échecs, le go, le chogi, l'hexagone, et constituent l'état de l'art actuel.

## L'intelligence artificielle au service de NTW

Par rapport aux échecs, NTW se caractérise par un facteur de ramification nettement plus important, mais en même temps une profondeur de recherche plus faible. Le facteur de ramification reflète approximativement le nombre d'actions raisonnables. Dans le cas de la NTW, plusieurs types d'actions sont possibles, y compris les coups, les attaques et les actions de réponse. En outre, à chaque tour de NTW, toutes les figures d'un joueur peuvent agir, contrairement aux échecs, où une seule figure se déplace. Ce résultat est un facteur de ramification de 50 à 100 en général. D'autre part, la profondeur de jeu est limitée pour chaque scénario, la profondeur standard étant de 12, ce qui est beaucoup plus petit que pour les échecs.

En raison de l'importance du facteur de ramification, les IA prêtes à l'emploi pour les environnements AlphaBeta ou MCTS ne peuvent être considérées pour NTW qui nécessite donc une approche personnalisée. Une particularité du jeu réside notamment dans la possibilité d'actions de réponse directes à une action de l'adversaire sans attendre le tour suivant, ce qui brise les ordres de mouvement standard des jeux stratégiques décrits ci-dessus. Une IA expérimentale est actuellement mise en œuvre dans l'environnement open source PyTorch (par Facebook). Les expériences sont menées avec plusieurs agents afin de mesurer leurs performances sur NTW. L'agent artificiel peut jouer contre des utilisateurs humains via une interface web (Figure 6).

## Un compagnon numérique

Disposant à ce stade de données sur tous les résultats possibles du jeu et des Intelligences Artificielles capables d'y jouer, nous devrions être en mesure d'aider le joueur à prendre la meilleure décision. Nous savons que dans la vie réelle, la situation serait différente, mais nous serions tout de même intéressés de simuler ce que pourrait être un « compagnon numérique » afin de mieux comprendre comment le biais cognitif du joueur apparaît lors du jeu. À cette fin, nous avons développé un simple jeu vidéo de NTW (Figure 7).

Le joueur incarne le soldat sur le terrain. Le défi consiste à reprendre certaines des situations initiales créées pour le jeu de plateau et à transformer le parcours de jeu en un récit pédagogique. Nous voulons ainsi apporter un éclairage supplémentaire aux questions soulevées par l'utilisation des nouvelles technologies.

Ces récits demanderont toujours au joueur de trouver l'utilisation optimale des nouveaux systèmes présents dans NTW : drone, exosquelette, robot de livraison armé et robot de rapatriement des blessés.

Comme les smartphones peuvent déjà être considérés comme nos « compagnons » quotidiens, le jeu est développé pour les appareils Android et Apple.

## Principe du jeu

Alors que les situations initiales sont basées sur les missions du jeu de plateau, nous utilisons les données fournies par les simulations multi-agents pour définir un nombre limité de progressions possible (par exemple, chemin de *réussite complet, chemin de réussite mixte*, chemin d'échec). Ces données forment un arbre narratif composé de différentes branches. A chaque nœud, le joueur choisit parmi une liste d'actions celle qu'il souhaite poursuivre.

## Un jeu instructif

Lors de la sélection d'une mission, la situation est décrite et accompagnée d'une illustration narrative. Un choix est alors proposé au joueur (par exemple, avancer / activer l'exosquelette / attendre). En fonction du choix, la situation suivante est présentée, suivie à nouveau d'un autre choix. Après avoir répété cette séquence plusieurs fois un résultat de mission est affiché. Le joueur sera d'abord invité à sélectionner (parmi un choix limité) les

raisons qui ont motivé sa décision. Ces données seront envoyées à un service d'analyse en ligne afin d'être interprétées.

Enfin, les choix du joueur seront représentés graphiquement, accompagnés d'un commentaire critique basé sur le parcours idéal. L'objectif est de permettre au joueur de comprendre ses erreurs.

Une fois la mission terminée avec succès, une nouvelle mission sera débloquée et deviendra jouable.

**Un compagnon pas toujours fiable**

Lors des premières missions, les joueurs/soldats devront prendre des décisions basées sur leur seul jugement. Le compagnon ne sera présent que pour commenter les situations décrites dans le jeu, pour donner des informations globales sur les événements en cours et pour fournir un retour d'information sur la fin du jeu.

Ce n'est qu'après quelques missions que le compagnon commencera à suggérer la voie optimale. Le but de cette mécanique de jeu est d'habituer lentement le joueur à recevoir de l'aide dans son processus décisionnel.

Cependant, pour les dernières missions, le compagnon commencera à suggérer de mauvaises options, ce qui entraînera l'échec de la mission si le joueur la suit. L'approche narrative justifiera cela par un piratage informatique et mettra en avant le fait que votre fidèle compagnon numérique, aussi sympathique et attachant soit-il devenu, peut lui-aussi être soumis à des attaques cybernétiques. Garder l'esprit critique peut sauver votre vie digitale !

**Conclusion et vision**

Tous les éléments présentés dans cet article interagissent avec pour simple objectif de répondre à la question « Comment puis-je faire l'expérience de quelque chose, si ce quelque chose n'existe pas ? ». Dans le contexte présent, le chose en question est une nouvelle technologie ou un produit résultant de l'intégration de celle-ci.

En parallèle à l'identification de ces technologies et au suivi de leurs évolutions, il incombe également à la prospective de tenter d'expliquer les conséquences et implications de l'utilisation de celles-ci. Permettre à la personne intéressée de se projeter dans le futur par l'intermédiaire du jeu sérieux favorise la compréhension de ce que permettraient ces nouveaux produits.

Le passage au format digital rend possible l'utilisation ~~de~~ d'intelligences artificielles fournissant au joueur la prise de connaissance de nouvelles options tout en le rendant attentif à ses biais cognitifs potentiels et aux risques qu'ils occasionnent.

Comme ces quelques pages en témoignent, nous sommes au début de cette aventure et des efforts sont encore nécessaires dans de nombreuses directions avant de


Copies d'écran du jeu vidéo « Le compagnon du soldat » se focalisant sur l'aide à la décision et l'interface homme-machine et considérant les mêmes scénarios que ceux utilisés dans le jeu de plateau.

pouvoir généraliser certaines conclusions et valider certaines intuitions. Le voyage s'annonce passionnant et prometteur dans ce qui se présente comme la construction d'un écosystème physique et numérique de prospective technologique dont les interactions entre les deux mondes permettent de mieux comprendre et anticiper ce que les nouvelles technologies nous réservent.

Restez à l'écoute…

Q. L. & M. R.

La rédaction de cet article a été rendue possible grâce au travail et aux contributions des personnes suivantes : «New Techno War» par Helvetia Games SA (Pierre-Yves ~~Frnzetti~~) ; simulations multi-agents par Scensei GmbH (Armando ~~Celle~~, Maciej M. Latek) ; Intelligence Artificielle par l'Istituto Dalle Molle di Studi sul'Intelligenza Artificiale (Oleg Szehr, Claudio Bonesana et Alessandro Antonucci) ; Jeu Vidéo «The Soldier's Companion» par Oni3 SNC (Mathieu Pellet, Seiko Annie Rubattel et Nicolas Schluchter)

**Liens :**

deftech.ch (*Prospective technologique*) sicherheitsforschung.ch (*Recherche auprès d'armasuisse*) armasuisse.ch/wt (*armasuisse Sciences + Technologies*)

# Never Home

# CAESAR®

The Caesar® artillery system in Mali

Photo credits: ©ECPAD/France/A.Roine

**CREATING REFERENCES IN DEFENSE**

nexter A COMPANY OF KNDS

Figure 1 : Organigramme du DTA avec indication du nombre d'EPT et de collaborateurs ainsi que des domaines de compétence respectifs

*210*

## Centre de compétence…

**Simon Baechler, Sami Hafsi, Ivan Keller**

Commissaire principal, chef du Domaine Traces et Analyse criminelle, Police judiciaire, Police neuchâteloise
Commissaire divisionnaire, chef de la police judiciaire, Police neuchâteloise
Lieutenant-colonel, chef d'état-major, Police neuchâteloise

# COMMUNICATION SÉCURISÉE ET MONITORING SONT UNE QUESTION DE CONFIANCE

Roschi Rohde&Schwarz SA vous soutient en tant qu'entrepreneur général avec une expertise locale dans le maintien de votre souveraineté numérique.

**www.rohde-schwarz.com/ch**

ROHDE&SCHWARZ
Make ideas real


Le Centre de politique de sécurité, Genève (GCSP) est un centre de formation international dédié aux questions de sécurité. Fondation internationale comptant 45 Etats membres, le centre offre des cours pour des décideurs d'administrations nationales et du secteur privé et associatif. Par la recherche et l'organisation de conférences, le GCSP favorise la réflexion et le dialogue sur les grands thèmes de sécurité internationale.

*Cyberdéfense*

# Le « Cyber 9/12 Strategy Challenge » – Une simulation de crise digitale pour les experts de cyber-securité de demain

**Dr. Robert S. Dewar**
Head of Cyber Security and Director of the Cyber 9/12 Strategy Challenge (Geneva), Geneva Centre for Security Policy

Cette année, le Centre de Politique de Sécurité de Genève (GCSP) célèbre son 25e anniversaire. Les 2 et 3 juillet 2020, le GCSP a accueilli la 6e édition de l'étape genevoise du Cyber 9/12 Strategy Challenge. Organisé en partenariat avec l'Atlantic Council (AC), le GCSP a accueilli des étudiants du monde entier, notamment de Suisse, d'Estonie, du Royaume-Uni, de Finlande, Norvège, France, des Etats-Unis et d'Inde. Vingt équipes se sont affrontées pour être couronnés champions de la compétition. attribuée à l'équipe PromETHeus de l'ETH Zurich, après un round final entièrement disputé par des équipes de l'ETH ! Le premier prix a été annoncé et décerné par S.E. M. Andrew Bremberg, représentant permanent des Etats-Unis d'Amérique auprès de l'Of-fice des Nations Unies et des autres organisations internationales à Genève, et l'ambassadeur Christian Dussey, directeur du GCSP.

Cette année, la compétition a accueilli pour la première fois une équipe d'Inde. C'est aussi la première fois que l'événement s'est déroulé entièrement virtuellement, en utilisant des plateformes de conférence en ligne pour permettre aux participants de participer depuis n'importe où dans le monde.

## Contexte de la Competition

Le Cyber 9/12 Strategy Challenge est ne série de compétitions annuelles de développement de recom-mandations politiques et stratégiques organisées dans le monde entier. Les compétitions mettent les participants au défi de créer des solutions et des recommandations politiques innovantes en réponse à un incident de cybersécurité fictif et évolutif. Cette année, les équipes devaient faire face à une crise affectant l'approvisionnement des infrastructures énergétiques essentielles d'un un pays fictif. Aux premiers abords, le scénario laissai entendre que l'incident pourrait avoir été commandité par un Etat. Au fur et à mesure que le scénario se développait, le cyber-incident fictif semblait en effet être un prélude à une invasion. Il s'avère ensuite que l'incident résulte de l'acte d'un seul employé mécontent qui avait récemment été licencié. Des équipes prenant part dans la compétition ont dû donc faire face à la complexité liée au fait d'avoir d'abord recommandé des politiques militaires pour ensuite devoir désamorcer la situation pour éviter un conflit.

Le Cyber 9/12 Strategy Challenge est une compétition rendue unique précisément grâce à l'accent mis sur le développement de recommandations politiques et stratégiques. Il existe en effet de nombreux événement se focalisant sur la partie technique de la cybersécurité. On pense notamment au « Hackathons ». En revanche, le Cyber 9/12 Strategy Challenge est spécifiquement conçu pour le développement et l'étude de solutions politiques et géostratégiques. Il n'est pas nécessaire d'avoir une formation technique pour y participer.

La série des Cyber 9/12 Strategy Challenge est coordonnée par L'Atlantic Council, basé à Washington, D.C. Créé en 2012 par Jason Healey alors qu'il était directeur de la Cyber Statecraft Initiative au Atlantic Council, le Challenge a été conçu dès le départ comme un événement destiné aux étudiants. Toute personne inscrite à un cours universitaire peut y participer.

Alors que la compétition initiale était un événement annuel unique destiné aux étudiants américains, le Challenge s'est développé au fur et à mesure des années, et englobe aujourd'hui sept événements indépendants dans le monde entier. Les Cyber 9/12 Strategy Challenges se déroulent maintenant à Londres (Royaume-Uni), Lille (France), Genève (Suisse) et Canberra (Australie) ainsi que des compétitions américaines à Austin (Texas), New York et Washington. Cela a créé une « saison » 9/12, avec tous les concours se déroulant au cours de l'année civile universitaire de septembre à mai, afin de garantir que tous les étudiants bénéficient du plus grand soutien de leur faculté.

Briefing des juges du Cyber 9/12 Strategy Challenge.

Les juges du Cyber 9/12 Strategy Challenge écoutent une présentation du concours.

**Qui soutient la compétition ?**

Depuis sa création, la compétition repose sur le soutien du secteur public et du secteur privé. Toutefois, au fil des années, le niveau d'engagement a augmenté de manière exponentielle. Parmi les entreprises qui le parrainent et le soutiennent, on trouve de grands conglomérats internationaux tels que Facebook, Kudelski, KPMG et FireEye.

La compétition a également bénéficié d'un soutien important des gouvernements du Royaume-Uni, de la Finlande, de l'Estonie, de l'Australie, de la France et de la Suisse. Pour la compétition de 2020, nous avons accueilli le soutien de la Mission des Etats-Unis à Genève.

**Comment la compétition se déroule-t-elle ?**

Sur deux jours, la compétition exige des participants qu'ils réagissent à un incident de cyber sécurité de plus en plus grave.
Les incidents abordés dans le cadre des compétitions sont nombreux et variés. À ce jour, ils ont porté sur des questions aussi diverses que le piratage des systèmes de contrôle du trafic aérien, les défaillances systémiques des réseaux de navigation maritime et de contrôle des autorités portuaires, l'exploitation des capacités militaires de commandement et de contrôle ou les opérations de rançon contre des entreprises civiles de télécommunications. Ces incidents fictifs sont d'abord localisés, mais ils ont un impact et une ampleur suffisants pour justifier une enquête par un groupe de travail (fictif) composé de représentants des États membres européens.
Dans les semaines avant la compétition, les équipes reçoivent un « Intelligence Brief ». Il s'agit d'un ensemble d'articles de presse, de rapports officiels, de dossiers de renseignements et de publications sur les réseaux sociaux - tous entièrement fictifs - contenant des détails sur l'incident. Une fois sur place, le premier jour de la compétition, toutes les équipes présentent leurs recommandations en réponse aux informations contenues dans le dossier de renseignement à un jury. Les juges jouent le rôle des chefs d'Etat et de gouvernements convoqués pour traiter de la crise.

Les équipes sont tenues de présenter des options politiques pour faire face a la crise, et de faire une recommandation. Elles sont jugées non seulement sur leurs compétences en matière de présentation, mais aussi sur leur compréhension de la situation, leur maîtrise de la politique de cybersécurité et leur compréhension du contexte géopolitique dans lequel l'incident fictif se déroule. Non seulement les juges défient les concurrents en demandant des justifications pour leurs recommandations politiques, mais ils fournissent également un retour sur ces recommandations d'un point de vue professionnel et réel. Ces juges attribuent des points pour les présentations, les équipes ayant obtenu les meilleurs scores accédant à la demi-finale le matin du deuxième jour.

Le soir du premier jour, les équipes qui sont avancées aux demi-finales reçoivent un deuxième « Intelligence Brief » décrivant une intensification de la crise et travaillent toute la nuit afin de préparer leur présentation pour la demi-finale. Cela implique souvent que les équipes travaillent toute la nuit sur leur recommandation !

Lors des demi-finales, les équipes présentent à nouveau devant un panel d'experts, et quatre équipes sont sélectionnées pour participer à la finale. En finale, les équipes reçoivent le troisième et dernier « Intelligence Brief » décrivant une nouvelle intensification de la crise et disposent de 30 minutes pour préparer leurs réponses avant de présenter pour la dernière fois devant un panel d'experts.

**Les équipes**

Pour participer au Cyber 9/12 Strategy Challenge en tant que concurrent, les participants doivent être inscrits à un cours universitaire au moment de l'inscription. Les équipes sont souvent constitués d'étudiants de niveau Bachelor, ainsi que de Mater et de Doctorat.

Être inscrit à un programme universitaire scientifique ou informatique n'est pas requis pour participer à la compétition. Au contraire, nous encourageons la participation d'étudiants de sciences politiques, pour apporter une manière de penser nouvelle et innovante a


Les équipes se préparent à participer au Cyber 9/12 Strategy Challenge.

des problèmes techniques. Nous permettons ainsi une interaction directe entre la politique sociale et l'expertise technique. Ce mélange aide les législateurs, les décideurs politiques et les dirigeants de demain à aborder la cybersécurité et la politique digitale avec une perspective plus globale, en encourageant des solutions plus créatives. Le Cyber 9/12 Strategy Challenge est un « sport d'équipe ». Les participants ne peuvent donc pas y prendre parts tout seules, mais doivent faire partie d'une équipe de 4. Il est aussi nécessaire d'avoir un coach. Les coaches peuvent être des professeurs d'université, professionnels de l'informatique, anciens fonctionnaires. Leur rôle est de guider les équipes dans les phases de préparation et de compétition. Pour éviter de donner un avantage aux participants provenant d'institutions avec plus de ressources, les équipes ne peuvent que constater leur coach durant la compétition. Recevoir de l 'aide extérieur est interdit.

Les équipes viennent du monde entier pour participer. Les participants réguliers à la compétition de Genève sont l'Université de Saint-Gall, l'ETH Zurich, l'EPFL Lausanne, U.S Military Academy at West Point et le U.S Naval College des États-Unis et l'Université de Glasgow. Cette diversité de participation est retrouvée dans la diversité des solutions présentés durant la compétition, du fait des différents contextes culturels et régionaux des différentes équipes.

**Comment la compétition est-elle jugée ?**

Les juges sont tout aussi importants pour la compétition que les participants eux-mêmes. Les juges des sept événements annuels de Cyber 9/12 sont issus de nombreux horizons. Ils sont des représentants du monde universitaire, des diplomates actuels et anciens, des fonctionnaires de carrière travaillant dans des organisations nationales et régionales, des professionnels du secteur de la cybersécurité et des représentants de la société civile. Tous ont une grande expérience de la cybersécurité. Ils donnent de leur temps et mettent leur expertise et leur expérience au service de la compétition afin de juger les réponses des participants mais aussi de donner un aperçu des processus décisionnels réels. De nombreux juges ont été appelés à proposer des options politiques dans des cybercrises réelles et connaissent bien les processus politiques et juridiques complexes nécessaires pour réagir de manière efficace et opportune à une crise.

Cette interaction entre les étudiants et les professionnels de la cyber-sécurité est vitale car elle aide les participants à faire la différence entre la fiction, et la réalité de la gestion nationale, régionale et mondiale de la cybersécurité. Cette expérience permet d'informer les futurs dirigeants sur les réalités et les aspects pratiques de la conception de solutions politiques de cybersécurité, ou sur les cadres juridiques, réglementaires et civiques dans lesquels les gouvernements, l'industrie et la société doivent opérer. Une telle expérience est cruciale pour un monde numérique plus sûr.

**De plus...**

Le Cyber 9/12 Strategy Challenge n'est pas seulement l'occasion pour les élèves de se mesurer à une cyber-crise en pleine évolution. C'est aussi une occasion inestimable de « networking » pour les participants et les juges. En plus de la compétition, des événements parallèles tels que des séances d'orientation professionnelle, des panels de haut niveau discutant des derniers développements géopolitiques, des discours en plénière et des ateliers ont lieu. Ces derniers servent à créer une communauté de professionnels et d'experts afin d'avoir le plus grand impact possible sur le monde numérique d'aujourd'hui.

Ces occasions pour les étudiants s de rencontrer et d'interagir avec des professionnels et des experts de haut niveau issus des mondes techniques et politiques sont inestimables et peuvent fournir des informations utiles aux étudiants dans leurs domaines de prédilection. Elles permettent également aux juges de rencontrer la prochaine génération de talents dans le domaine de la cybersécurité. Un certain nombre de concurrents proches de la fin de leurs études ont obtenu des stages et des contrats de travail grâce aux contacts établis lors du Challenge.

**L'impact du COVID-19 sur la compétition 2020 à Genève**

En 2020, le Cyber 9/12 Strategy Challenge a pris une tournure inattendue. Dans des circonstances normales, le GCSP accueille plus de 300 personnes à la Maison de la paix pendant deux jours de séminaires, de concours, de discussions, de plénières et de séances de networking. La pandémie mondiale de COVID-19 a fait que la compétition normale ne pouvait pas se dérouler en toute sécurité.

En discussion avec nos partenaires de L'Atlantic Council, le GSCP a choisi d'organiser une compétition virtuelle. Tirant parti de notre propre expérience croissante dans l'organisation de grands événements en ligne et de celle de L'Atlantic Council qui a organisé une compétition virtuelle plus tôt dans l'année à Washington DC, le GCSP a converti le format du Challenge en une expérience entièrement en ligne. Les équipes ont présenté leurs recommandations aux juges par vidéoconférence depuis le monde entier, et les sessions plénières, les discours et les événements parallèles ont tous été organisés en ligne.

La conversion numérique a été bien accueillie par les participants et les juges. Bien que les possibilités de réseautage aient été limitées en raison du manque d'interaction physique, les sessions du Challenge elles-mêmes, ainsi que la série d'événements parallèles proposés, ont permis aux élèves de continuer à participer, à s'engager et à discuter des derniers développements cybernétiques avec les juges. Un panel de haut niveau impliquant S.E. M. Andrew Bremberg (représentant permanent des Etats-Unis d'Amérique auprès de l'Office des Nations unies et d'autres organisations internationales à Genève), Mme Chelsey Slack (chef adjoint de la cyberdéfense, OTAN), le Dr Trey Herr (directeur de la Cyber Statecraft Initiative, Atlantic Council) et animé par le Dr Robert Dewar (chef de la cyber sécurité au GCSP et directeur du Geneva Cyber 9/12 Strategy Challenge) a réuni plus de 100 participants virtuels et a donné lieu à une discussion intéressante sur les derniers développements de la cyber diplomatie.

Le succès de la logistique considérable qu'a impliqué la coordination de plus de 200 appels individuels en ligne pendant deux jours témoigne du dévouement et du travail acharné de l'équipe du Cyber 9/12 du GCSP, ainsi que de l'agilité du GCSP à s'adapter à des événements soudains, inattendus et extrêmement importants. À la suite de ces expériences, le GCSP et le Atlantic Council apportent leur soutien à d'autres événements Cyber 9/12 dans le monde entier qui envisagent également de passer au format numérique. L'une des leçons tirées de cette conversion est qu'elle a ouvert la porte à la participation d'un plus grand nombre d'étudiants de pays plus lointains, et pas seulement du monde occidental. Ces compétitions deviennent de véritables affaires mondiales.

**Qu'est-ce que le Cyber 9/12 Strategy Challenge apporte-t-il à la Suisse?**

Les équipes des universités suisses ont toujours été des concurrents réguliers du Cyber 9/12 de Genève, et ont historiquement obtenu de très bons résultats. Cette année, cependant, la représentation suisse a connu une année exceptionnelle face à une forte cohorte internationale. Les équipes de l'ETH Zurich ont pris les cinq premières places du classement. L'expérience des institutions universitaires suisses s'est développée ces dernières années pour comprendre non seulement l'interrelation entre la politique de cybersécurité et les solutions techniques, mais aussi comment placer ces solutions dans un contexte géopolitique et géostratégique plus large. La plupart des étudiants des équipes des institutions suisses, mais pas tous, sont eux-mêmes suisses. Ils sont les futurs experts, législateurs et dirigeants de la Suisse en matière de cybersécurité. En participant au Cyber 9/12 et en faisant face à des équipes du monde entier ils élargissent leur base de connaissances et leur expérience, ce qui leur permettra d'élargir leur perspective au-delà des processus européens de résolution de problèmes. Les défis auxquels nous sommes confrontés aujourd'hui ne nous sont pas propres. Mais en apprenant comment d'autres parties du monde font face à ces mêmes défis, les futurs experts suisses aborderont ces défis de manière nouvelle et créative.

La tenue de l'un des sept défis à Genève renforce également la position internationale de la Suisse en tant que centre de *leadership* créatif dans le domaine de la cybersécurité. La Genève internationale est déjà un centre dynamique pour la politique numérique. Mais le Cyber 9/12 Strategy Challenge sert de point de rencontre - un lien - pour les experts et professionnels techniques, juridiques, sociaux et politiques. C'est l'occasion de rencontrer et de dialoguer avec des représentants de tous les secteurs nécessaires à la réalisation d'un monde plus sûr sur le plan numérique. L'itération genevoise de la compétition bénéficie déjà d'un excellent soutien de la part du gouvernement suisse, mais nous espérons que ce soutien se poursuivra et s'élargira.

Le Cyber 9/12 Strategy Challenge est un investissement unique dans l'avenir de la Suisse, à la fois en termes de soutien aux jeunes qui y participent, mais aussi en termes de facilitation du partage d'idées et d'expériences entre les professionnels de première ligne actuels et anciens. Le Challenge a donc un impact significatif sur l'élaboration des politiques internationales en matière de cybersécurité dans de nombreux domaines. En raison de la diversité des thèmes abordés dans les scénarios - de la sécurité aérienne à la sécurité maritime en passant par l'approvisionnement en énergie -, il a un impact sur l'élaboration de la politique de cybersécurité dans toute une série de domaines politiques. Les professionnels qui jugent les équipes

considèrent le Challenge comme un banc d'essai pour des solutions créatives à certains des défis les plus complexes auxquels nous sommes confrontés aujourd'hui en matière de cybersécurité. Le Challenge n'est donc pas un simple concours d'étudiants : c'est un centre de réflexion créative et d'élaboration de solutions.

## Conclusion

Au fil des ans, le Cyber 9/12 Strategy Challenge de Genève a pris de l'ampleur et s'est heurté à des obstacles logistiques uniques. Cette année, le COVID-19 a obligé les organisateurs à se lancer dans l'inconnu et à organiser une compétition internationale de grande envergure totalement en ligne. Les évènements en ligne semblent destinés à faire partie de la vie quotidienne pendant un certain temps encore. Nous allons donc nous adapter à cette nouvelle normalité et espérons étendre la participation au Challenge encore plus loin. Nous attendons avec impatience ce que 2021 nous apportera.

R. D.

**Liens**

Cyber 9/12 Strategy Challenge in Geneva, Switzerland
Atlantic Council Cyber 9/12 Strategy Challenge homepage

News

### Renforcement de la cyberdéfense

Berne, 07.10.2020 – Lors de sa séance du 7 octobre 2020, le Conseil fédéral a lancé la procédure de consultation portant sur diverses modifications touchant la loi sur l'armée, l'organisation de l'armée et d'autres bases légales. Il entend notamment créer un commandement Cyber et accroître les effectifs de milice dans ce domaine. Parmi les autres nouveautés notables, la mise en place d'une nouvelle autorité responsable du trafic aérien militaire pour assurer la sécurité des Forces aériennes ainsi qu'un renforcement de l'appui aux événements civils. La consultation prendra fin le 22 janvier 2021.

La mise en œuvre du processus développement de l'armée (DEVA) a débuté le 1er janvier 2018 et se terminera le 31 décembre 2022. D'emblée, il s'est avéré que des adaptations étaient nécessaires dans divers domaines, malgré les mesures internes de correction que l'armée a déjà prises et appliquées, pour partie. Certains de ces domaines exigent que la loi sur l'armée (LAAM), l'organisation de l'armée (OOrgA) et d'autres bases légales soient révisées.

**La Base d'aide au commandement deviendra le commandement Cyber en 2024**

En concrétisant le DEVA, il était prévu de subdiviser l'armée en trois domaines distincts : le commandement des Opérations, le commandement de l'Instruction et le commandement du Soutien, lui-même composé de la Base d'aide au commandement (BAC) et de la Base logistique de l'armée (BLA). En application de la motion 19.3427, que les Chambres fédérales ont adoptée lors de la session d'été 2020, décision a été prise de renoncer, dans le cadre de la révision LAAM/OOrgA, à mettre la BAC et la BLA sous un même commandement car il n'en résulte aucune possibilité d'optimisation par rapport à l'organisation actuelle.

Vu les menaces qui prédominent actuellement, le Conseil fédéral entend transformer la BAC en un commandement spécifique appelé commandement Cyber au début de 2024, ce qui nécessite une adaptation de l'OOrgA. La numérisation ainsi que la modernisation et la mise en réseau qui en résulteront de tous les systèmes de l'administration militaire et de l'armée progressent rapidement. Cette évolution soumet une architecture informatique uniformisée à de fortes exigences et exige une standardisation des applications. De plus, les processus croissants de mise en réseau augmentent sensiblement le nombre de défis à relever dans le domaine de la cyberprotection. Aussi, pour faire face du mieux possible à ces exigences, la BAC devra se transformer pour passer d'une organisation de soutien largement sectorisée à un commandement militaire strictement opérationnel.

Le commandement Cyber devra organiser les capacités militaires clés dans les domaines de l'image de la situation, de la cyberdéfense, des prestations informatiques, de l'aide au commandement, de la cryptologie et de la guerre électronique.

**Cyberinstruction à l'armée complétée en coopérant avec des externes**

Au niveau de l'armée également, il est prévu d'augmenter ces prochaines années l'effectif du personnel dans le domaine de la cyberdéfense avec la mise sur pied, le 1er janvier 2022, d'un cyberbataillon et d'un état-major spécialisé correspondant, faisant ainsi passer l'effectif actuel du personnel de milice, qui est de 206, à 575 militaires. Pour accroître également la qualité de l'instruction dispensée à ces cyberspécialistes au sein de l'armée, celle-ci sera complétée par un stage auprès de partenaires externes, permettant ainsi d'approfondir et d'étendre les capacités acquises et, au final, d'en faire bénéficier l'armée.

**Création d'une autorité du trafic aérien militaire et autres adaptations**

Jusqu'à présent, la Suisse ne dispose pas d'organisation comparable à l'Office fédéral de l'aviation civile pour le trafic aérien militaire. Des bases légales vont donc être créées pour une autorité du trafic aérien militaire. Celle-ci doit assurer la sécurité des Forces aériennes lors de leurs missions dans l'espace qu'elles partagent avec l'aviation civile. Elle veillera notamment à éviter tout incident ou accident dans cet espace et à garantir mieux encore la surveillance et la régulation du trafic aérien militaire. Une adaptation de la loi sur l'aviation s'impose donc.
Appui renforcé aux événements civils

Dans la foulée de la révision de la LAAM, le Conseil fédéral entend aussi renforcer l'appui apporté par l'armée aux événements civils. Cela commencera par un accroissement de la souplesse et des disponibilités de l'armée dans le sens où les recrues en phase d'instruction de base pourront, elles aussi, être engagées, et plus seulement les militaires en service long et ceux en cours de répétition. L'armée devra également pouvoir fournir des prestations dans un cadre limité lors d'événements d'importance nationale ou internationale, même sans en retirer un avantage majeur au niveau de son instruction ou de son entraînement. En introduisant cette disposition d'exception, le Conseil fédéral tient compte du fait que les événements considérés ne pourraient pas avoir lieu sans l'appui de l'armée.

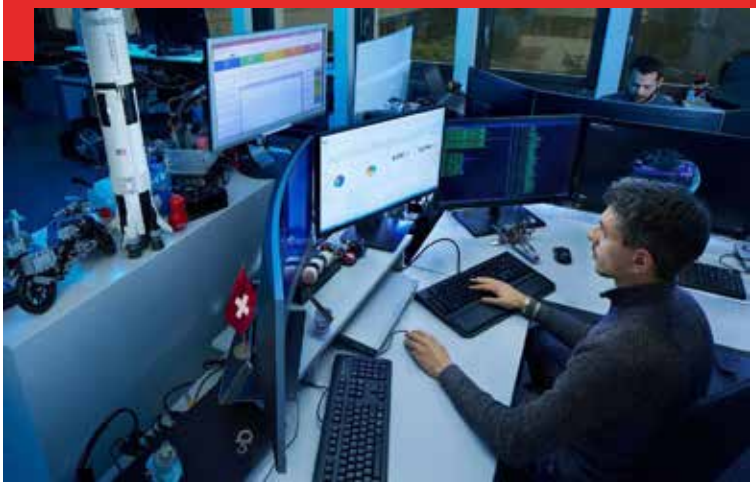
De surcroît, il est aussi nécessaire que le législateur intervienne dans certains autres domaines de l'instruction – celle des militaires en service long entre autres –, dans diverses dispositions sur l'engagement de l'armée en service d'appui, dans l'accomplissement des missions de l'armée en fonction des menaces dans le contexte actuel, dans les droits et les devoirs des militaires et dans le domaine des affaires sanitaires. Plusieurs dispositions de la LAAM doivent donc être modifiées. Enfin, l'appréciation lors du recrutement et lors de la remise de l'arme personnelle du potentiel de danger et d'abus que peuvent renfermer les militaires doit être améliorée.Jusqu'à présent, la Suisse ne dispose pas d'organisation comparable à l'Office fédéral de l'aviation civile pour le trafic aérien militaire. Des bases légales vont donc être créées pour une autorité du trafic aérien militaire. Celle-ci doit assurer la sécurité des Forces aériennes lors de leurs missions dans l'espace qu'elles partagent avec l'aviation civile. Elle veillera notamment à éviter tout incident ou accident dans cet espace et à garantir mieux encore la surveillance et la régulation du trafic aérien militaire. Une adaptation de la loi sur l'aviation s'impose donc.

**Appui renforcé aux événements civils**

Dans la foulée de la révision de la LAAM, le Conseil fédéral entend aussi renforcer l'appui apporté par l'armée aux événements civils. Cela commencera par un accroissement de la souplesse et des disponibilités de l'armée dans le sens où les recrues en phase d'instruction de base pourront, elles aussi, être engagées, et plus seulement les militaires en service long et ceux en cours de répétition. L'armée devra également pouvoir fournir des prestations dans un cadre limité lors d'événements d'importance nationale ou internationale, même sans en retirer un avantage majeur au niveau de son instruction ou de son entraînement. En introduisant cette disposition d'exception, le Conseil féwéral tient compte du fait que les événements considérés ne pourraient pas avoir lieu sans l'appui de l'armée.

De surcroît, il est aussi nécessaire que le législateur intervienne dans certains autres domaines de l'instruction – celle des militaires en service long entre autres –, dans diverses dispositions sur l'engagement de l'armée en service d'appui, dans l'accomplissement des missions de l'armée en fonction des menaces dans le contexte actuel, dans les droits et les devoirs des militaires et dans le domaine des affaires sanitaires. Plusieurs dispositions de la LAAM doivent donc être modifiées. Enfin, l'appréciation lors du recrutement et lors de la remise de l'arme personnelle du potentiel de danger et d'abus que peuvent renfermer les militaires doit être améliorée.

Source : https://www.vbs.admin.ch/content/vbs-internet/fr/die-aktuellsten-informationen-des-vbs/die-neusten-medienmitteilungen-des-vbs.detail.nsb.html/80621.html



L'Armée suisse dispose actuellement d'une infrastructure TIC (technologies de l'information et de la communication) hétérogène qui s'est développée au fil du temps. Certaines technologies encore utilisées de nos jours remontent à plusieurs décennies, tandis que le progrès technologique avance à un rythme effréné. Cette situation confronte la sécurité informatique à de grands défis, le fonctionnement et la sécurité de certains systèmes étant souvent en contradiction. Afin de remettre toutes ces infrastructures hétérogènes à niveau, des modifications fondamentales ont été décidées et entreprises ces dernières années pour moderniser l'informatique militaire.

*Cyberdéfense*

# La sécurité informatique est un processus et non pas un état

**Anna Muser**
Cheffe communication Base d'aide au commandement (BAC)

Au printemps 2018, l'ancien chef de la Base d'aide au commandement (BAC) a lancé un projet interne visant à accroître la sécurité des systèmes TIC de l'Armée suisse. L'élément déclencheur a été un incident lié à la cybersécurité qui s'est produit chez RUAG, mais aussi la découverte de failles dans les systèmes TIC de l'armée suite à des rapports, des tests et des essais d'intrusion. Des analyses toujours plus poussées ont révélé l'urgente nécessité d'agir. La mise en œuvre du projet se terminera dans un avenir proche. Cependant, afin de mettre en lumière le contexte actuel, un retour en arrière s'impose.

## L'histoire de la BAC

L'actuelle BAC existe en l'état depuis 2005. À l'époque, le Groupe de l'aide au commandement (Gr aide cdmt) a fusionné avec la Direction de l'informatique et de la communication (Dir infm DDPS). C'est aussi à cette époque que les systèmes informatiques militaire et civil du DDPS ont été fortement imbriqués. Les deux domaines avaient jusqu'alors poursuivi des objectifs totalement différents ; le personnel de ces entités avait des conceptions différentes de la sécurité, et les tâches à accomplir dans ces systèmes cloisonnés étaient difficilement conciliables. C'est à la fusion du Gr aide cdmt et de la Dir infm DDPS que l'on doit le fait que la BAC fournit aujourd'hui des prestations aussi bien pour le compte de l'armée et du Réseau national de sécurité (RNS) que de l'administration fédérale civile (DDPS ou autres départements).

En avril 2016, suite à l'incident survenu chez RUAG, Guy Parmelin, ancien chef du DDPS, a décidé de dissocier de nouveau les systèmes informatiques de l'armée et de l'administration. C'était là le seul moyen pour la BAC d'avoir une chance de parvenir à maîtriser des défis tels que l'adaptation au progrès technologique effréné, aux menaces croissantes dans le cyberespace et aux besoins de plus en plus importants de l'armée et de se concentrer sur sa mission de base.

## Dissociation de l'informatique civile et militaire

Dans le cadre du programme de dissociation des prestations informatiques de base, les systèmes de l'armée et du RNS revêtant une importance décisive pour l'engagement et posant des exigences élevées en termes de sécurité et de robustesse sont dûment séparés des systèmes de l'administration fédérale et fonctionneront, à l'avenir, de façon totalement autonome et distincte des systèmes civils. Le concept de dissociation prévoit que les systèmes militaires puissent échanger des informations de manière sûre et contrôlée avec le reste de l'administration fédérale et le monde civil. La dissociation des prestations informatiques de base et la création des nouvelles zones présentent trois avantages majeurs :

- La sécurité informatique des systèmes revêtant une importance décisive pour l'engagement sera considérablement accrue ;
- Les responsabilités pour la sécurité informatique seront clairement définies dans les différentes zones ;
- La BAC pourra se concentrer pleinement sur la fourniture de prestations pour l'armée et le RNS.

La fourniture des prestations de base, qui comprennent des dizaines d'application spécialisées civiles, devrait être déléguée au terme de la dissociation. Ainsi, l'ensemble de la bureautique pour quelque 15'000 utilisateurs sera transférée à l'Office fédéral de l'informatique et de la télécommunication (OFIT). Grâce aux économies d'échelle, les coûts informatiques pour l'administration seront réduits. Cette séparation des systèmes a déjà été réalisée depuis longtemps pour l'environnement hautement sécurisé du Centre des opérations électroniques, qui fournit des prestations dans le cyberespace et l'espace électromagnétique.

## Vers un système entièrement neuf

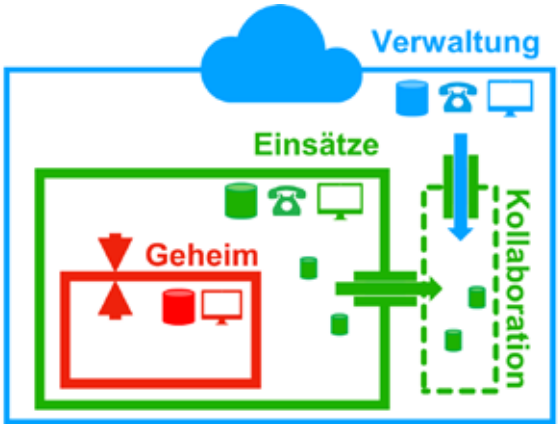
Afin de pouvoir réaliser la dissociation, une autre décision de principe était nécessaire. Soit l'on choisissait

Dans l'environnement de test du Réseau de conduite suisse, le contexte précédant la transition vers un système entièrement neuf est bien visible. Des câbles datant des années 1950 ... (© VBS/DDPS, photos: CME)

...cohabitent avec de la fibre optique moderne au sein de l'environnement informatique de l'Armée suisse.

de continuer d'utiliser les anciens systèmes pendant la dissociation, ce qui serait revenu à pratiquer une opération à cœur ouvert, soit l'on créait, parallèlement aux systèmes actuels, un système entièrement nouveau. En raison de la complexité de l'opération et des ressources disponibles, la deuxième solution a été retenue. L'ancien environnement informatique hétérogène sera donc abandonné pour laisser place à un système entièrement neuf.

De manière schématique, les différentes prestations informatiques au sein du DDPS sont décomposées en zones soumises à divers critères.




À cet égard, les prestations rassemblées dans le programme FITANIA constituent les fondements nécessaires. Avec l'adjudication du marché à Swisscom à l'automne 2019 pour la création de la plateforme des nouveaux centres de calcul, un partenaire industriel adéquat a été trouvé. Une approche moderne de la sécurité sera mise en œuvre d'emblée dans la nouvelle infrastructure informatique, ce qui permettra de garder constamment une vue d'ensemble des actifs informatiques et de garantir la continuité des services informatiques. Dans ce contexte, ce ne sont plus des systèmes individuels qui seront protégés, mais plutôt des informations. Certains systèmes anciens encore utilisés aujourd'hui mais qui ne satisfont plus aux exigences de sécurité actuelles ont déjà été isolés comme il se doit. Une extension de la protection informatique à des systèmes obsolètes ne serait pas viable économiquement. L'une des conséquences de cette façon de procéder est que les risques liés à ces systèmes isolés obsolètes sont sciemment supportés par le DDPS. De cette façon, les différences de ces systèmes vis-à-vis des principes de protection de base de la Confédération ne sont pas rapportées à l'Unité de pilotage informatique de la Confédération (UPIC), pourvu qu'elles ne mettent pas en péril les systèmes informatiques de la Confédération. Une annonce à l'UPIC aurait, en soi, entraîné des risques de sécurité.

## La question de la gouvernance

L'ordonnance sur l'informatique dans l'administration fédérale (OIAF) règle la gouvernance informatique dans l'administration fédérale, l'UPIC étant l'organe compétent dans ce domaine. Le Contrôle fédéral des finances (CDF) réalise les audits et maintient une vue d'ensemble des systèmes informatiques. Les différentes applications fournies par la BAC doivent toutefois satisfaire à des exigences de sécurité particulièrement élevées. Ainsi par exemple, les directives de sécurité des systèmes militaires sont très complètes, notamment dans les domaines de la protection et de la défense contre les menaces du cyberespace. La sécurité des systèmes militaires doit donc être vérifiée en utilisant un catalogue de critères étendu. À cette fin, un système de gestion de la sécurité de l'information (*Information Security Management System*, ISMS) spécifique a été mis en place à la BAC. Fin 2018, l'ISMS de la BAC a reçu la certification ISO/IEC 27001 de la SQS.

Grâce à la mise en œuvre conséquente de la dissociation, le DDPS assume d'ores et déjà la responsabilité de ses propres systèmes ainsi que les risques en résultant. Les directives de l'UPIC relatives aux principes de protection de base de la Confédération sont ainsi dûment appliquées, voire renforcées si nécessaire. Dans certains cas, il est néanmoins tout à fait possible que ces directives ne puissent être respectées pour les systèmes militaires, et ce pour des raisons techniques. Par exemple, l'authentification à deux facteurs ne peut pas être intégrée sur d'anciens systèmes produits par des fabricants tiers.

Le centre de calcul de Frauenfeld est l'un des éléments visibles du programme FITANIA, avec lequel la future infrastructure numérique de l'armée sera réalisée.

## En plein processus

En raison de la complexité des systèmes existants, il est impossible de mettre en place du jour au lendemain un environnement informatique robuste et hautement sécurisé pour l'Armée suisse. Les processus d'acquisition de l'administration fédérale, les ressources disponibles et les exigences auxquelles la BAC est actuellement soumise ont une influence notable sur le calendrier de mise en œuvre. Depuis 2018 et sa réorientation stratégique, la BAC tout entière se mobilise pour fournir des prestations informatiques et des opérations électroniques robustes et hautement sécurisées en toutes circonstances au bénéfice de l'Armée suisse. Afin d'identifier le niveau de sécurité dans la transformation en cours, plusieurs tests ont été réalisés à l'été 2018 avec des partenaires issus de l'industrie. Les résultats obtenus ont déjà permis d'augmenter considérablement la sécurité contre d'éventuelles manipulations indésirables et intrusions. De plus, un nouveau projet visant à automatiser la configuration des pare-feu a été lancé. De cette manière, les facteurs d'erreur humains ont pu être réduits au strict minimum, et l'état des différents composants peut être contrôlé facilement en tout temps.

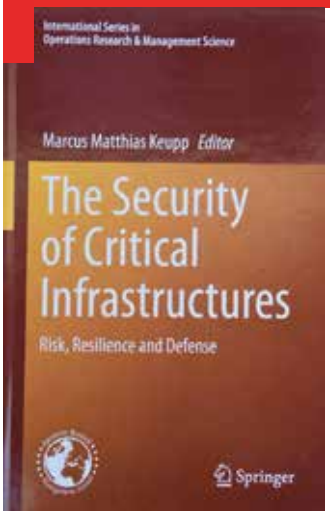
De nouvelles directives de sécurité architectoniques s'appliquent désormais aux systèmes existants; ces directives seront également appliquées aux futurs projets. À cet égard, une nouvelle structuration des systèmes de logiciels et des plateformes sur lesquelles ceux-ci reposent a été mise en place. L'une des mesures phare est la création du domaine Cyber Security et du poste de chef Cyber Security (CISO BAC). Les forces de sécurité de la BAC sont désormais concentrées dans ce nouveau domaine, qui regroupe les sections Stratégie de sécurité et Sécurité intégrale, ainsi que le Cyber Fusion Center. Ce dernier rassemble toutes les informations issues du cyberespace afin d'accroître le contrôle de la sécurité. Ceci permet en effet d'augmenter la surveillance des activités réseau. Une équipe Formation et *awareness* en matière de cybersécurité a été créée spécialement pour former les collaborateurs internes et externes de la BAC; cette équipe gère des modules d'apprentissage en ligne ainsi que des formations physiques afin d'accroître la sécurité. Par ailleurs, depuis le début de 2020, la BAC dispose aussi de l'*ICT Warrior Academy*, où des spécialistes sont formés aux nouvelles exigences de l'armée et reçoivent de nouvelles compétences. Dans le domaine Renouvellement, des méthodes agiles sont développées pour accroître la transparence, réagir plus rapidement aux exigences des clients et intégrer précocement les dernières technologies. En outre, en se concentrant sur la dissociation et la finalisation de FITANIA, des éléments garantissant une importante amélioration de la sécurité informatique seront mis en place au cours des prochaines années.

## Développement du commandement Cyber

Il s'agira dorénavant de pouvoir utiliser les moyens de l'armée avec précision en s'appuyant sur une avancée des connaissances et en anticipant les décisions. C'est pourquoi un réseau numérique souple formé de capteurs et d'effecteurs est nécessaire, permettant au commandant de prendre plus rapidement les bonnes décisions. Les capacités dans ce domaine doivent être encore davantage regroupées pour faire face aux menaces de plus en plus élevées, tant quantitativement que qualitativement. Dans le cadre de la motion Dittli de mars 2018, le Parlement a demandé le développement de la BAC en un commandement Cyber. Il s'agit en outre de la suite logique du développement de la BAC dans le cadre des objectifs 2030+ de l'Armée suisse. Le projet est actuellement dans sa phase d'initialisation, et une adaptation nécessaire de la loi sur l'armée est prévue. Afin de pouvoir garantir des prestations informatiques et des opérations électroniques robustes et hautement sécurisées en toutes circonstances au bénéfice de l'armée, la BAC a avant tout besoin de conditions stables et d'une endurance à toute épreuve.

A. M.

Article reproduit avec l'aimable autorisation de la Communication Défense




Le dernier livre édité par la chaire d'économie militaire publié chez Springer est consacré à la protection des infrastructures critiques de manière globale avec une approche scientifique.

*Economie de défense*

## La chaire d'économie militaire de l'ACAMIL se tourne vers la cyberdéfense

**Kilian Cuche**
Collaborateur de projet cyber à la chaire Economie de défense de l'ACAMIL à l'EPF de Zurich.

La chaire d'économie militaire de l'ACAMIL à l'EPF de Zurich, sous la direction du professeur Marcus Keupp, étoffe son *portfolio* de recherche avec des thématiques liées à la cyberdéfense, à la guerre économique et à la protection des infrastructures critiques. En effet, au vu de l'augmentation des menaces hybrides, il est devenu primordial d'axer également la recherche en économie de défense sur ces thématiques afin de contribuer à la résilience des forces armées. Ces nouvelles recherches permettent d'apporter une vue économique et managériale sur des thématiques souvent abordées uniquement dans leur aspect technique. Nos homologues français produisent également des recherches économiques sur ces thématiques, notamment au sujet de l'industrie et l'innovation de défense comme présenté dans une publication récente de la *Revue Défense Nationale* (RDN).[1]

Méthodiquement, la chaire est tout d'abord focalisée sur l'économie institutionnelle ainsi que l'analyse économique des prescriptions légales et des règlements. Elle analyse l'organisation militaire d'un point de vue institutionnel afin d'examiner les possibilités et les limites de l'action économique au sein de ces organisations. Des analyses économiques et de gestion permettent de rattacher les problématiques économiques militaires à des aspects institutionnels et de performance. Ces dernières aboutissent dans des recommandations en matière de conception institutionnelle pour la pratique organisationnelle des organisations militaires.

La chaire se concentre aussi sur la recherche qui contribue à améliorer la sécurité de l'Etat et de la société. Elle analyse les techniques de la guerre économique moderne[2] ainsi que la gestion stratégique des technologies et de l'innovation. La résilience des infrastructures critiques est également évaluée par la simulation et l'analyse quantitative. De plus, deux recherches ont été menées dans le domaine de l'économie de la cybersécurité. L'analyse de ces différents domaines révèle des vulnérabilités stratégiques et contribue ainsi au développement des stratégies de défense contre les attaques hybrides. Finalement, des nouvelles publications ainsi que deux projets de recherches dans le domaine de la cyberdéfense sont en cours.

### Economie militaire

Deux ouvrages phares ont été publiés par la chaire dans le domaine de l'économie de défense. Le premier concerne le passage stratégique de la Route de la Mer du Nord (publié en 2015 chez Springer[3]). Ce livre aborde les défis stratégiques, économiques, logistiques, judiciaires et militaires du futur grand jeu politico-stratégique dans la mer arctique. En effet, le changement climatique mondial a ouvert une nouvelle route maritime en Mer du Nord qui se propose comme une alternative stratégique à la route de Suez. Ajoutez à cela la découverte de nombreux produits de base et métaux facilement extractibles dans la région arctique et vous obtenez une attention toute particulière de la part des dirigeants d'entreprises et des leaders militaires sur cette nouvelle route maritime.

Le deuxième, Economie Militaire (publié en 2019 chez Springer[4]), était purement consacré à l'analyse institutionnelle de l'organisation militaire. Cet ouvrage analyse les problématiques d'efficacité et d'efficience des forces armées organisée dans une économie planifiée et propose des solutions afin d'améliorer la performance économique de l'organisation militaire par l'introduction d'une décentralisation des droits de propriétés au niveau des unités.

1 Rademacher, Benoît (dir.) et Malizard, Julien (dir.), 2020. Economie de défense : problématiques contemporaines. Revue Défense Nationale, 832.

2 https://www.vtg.admin.ch/de/organisation/kdo-ausb/hka/milak.detail.news.html/vtg-internet/verwaltung/2016/16-09/16-09-10-milak.html

3 https://www.springer.com/gp/book/9783658040802

4 https://www.springer.com/gp/book/9783658252878

## Economie de la cybersécurité

Deux thèses de doctorat en systèmes d'information réalisée à HEC Lausanne ont débuté la réorientation stratégique de la chaire dans le domaine de la cyberdéfense. Ces travaux se concentrent sur les problématiques économiques de la cybersécurité. La première, réalisée par le Dr. Alain Mermoud porte sur l'économie comportementale appliquée à la sécurité des systèmes d'information.[5] Elle s'intéresse plus particulièrement au mécanisme incitatif permettant de favoriser le partage de l'information utile à la cybersécurité entre opérateurs d'infrastructures critiques. Cette thèse contient trois articles. Le premier présente un cadre théorique qui associe le comportement humain et les résultats du partage d'information. Le deuxième article développe et teste empiriquement ce modèle théorique. Le dernier article propose des recommandations politiques afin de réduire les coûts d'exécution du partage d'information cyber.

La deuxième thèse, réalisée par le Dr. Dimitri Percia David aborde l'économie et l'acquisition des ressources pour générer des capacités de cyberdéfense.[6] Elle est également réalisée en trois articles. Le premier est consacré aux ressources matérielles et démontre que les évolutions rapides dans le domaine technologique exigent de nouvelles hypothèses de modèle d'investissement. Cet article propose un modèle pour aider à anticiper l'effet des technologies de rupture sur le niveau optimal d'investissement en cyberdéfense. Il fournit également un cadre pour sélectionner et investir dans les technologies les plus efficaces. Le second est consacré aux ressources humaines et démontre qu'une organisation doit mettre l'accent sur le recrutement de fournisseurs de connaissances spécialisées afin de construire une capacité de cyberdéfense. Le dernier article est consacré aux ressources de connaissances et démontre que l'organisation doit encourager l'apprentissage continu de ses membres afin de construire une capacité de cyberdéfense efficace. Finalement, cette thèse propose des recommandations stratégiques à l'intention du gouvernement et des fournisseurs d'infrastructures critiques.

## Sécurité des infrastructures critiques

La chaire d'économie de défense a également chapeauté la publication d'un livre consacré à la sécurité des infrastructures critiques publié en 2020 chez Springer Nature.[7] Ce livre analyse la sécurité des infrastructures critiques comme les réseaux routiers, ferroviaires, d'eau, de santé et d'électricité qui sont vitaux pour la société et l'économie d'une nation. Il évalue la résilience de ces réseaux face aux attaques intentionnelles. Des experts en recherche et gestion des opérations, en économie, en analyse des risques et en gestion de la défense ont contribué à ce livre en présentant des analyses théoriques, des graphiques, des statistiques avancées ainsi que des méthodes de modélisation appliquées. Finalement, ce livre identifie et discute des implications pour l'évaluation des risques, la politique et l'assurabilité des infrastructures critiques. Les conclusions présentées dans cet ouvrage sont applicables à l'échelle mondiale et ne se limitent pas à des lieux, des pays ou des contextes particuliers.

De plus, Sébastien Gillard, qui a également contribué à ce livre avec deux chapitres poursuit sa recherche dans ce domaine. Actuellement, il apporte sa contribution à un projet orienté sur la protection des infrastructures critiques et l'investissement dans la sécurité de l'information, en partenariat avec le Cyber-Defence Campus d'armasuisse basé à l'EPFL. En parallèle, il prépare une autre recherche pour sa thèse de doctorat consacrée à l'optimisation de la *Cyber Threat Intelligence (CTI)* au moyen de méthodes éconophysiques.[8]

## Social Engineering

D'autres travaux dans le domaine de la cyberdéfense sont en cours d'élaboration. Une nouvelle thèse consacrée aux problématiques de *social engineering* (pratique de manipulation psychologique à des fins d'escroquerie en ligne) est également en cours de rédaction par Fabian Muhly en partenariat avec le département de criminologie de l'Université de Lausanne. Cette recherche vise à valider un instrument pour être plus à même de combattre les délits associés aux techniques de *social engineering*. Ce travail utilise le *Serious Gaming* comme un outil pour diminuer le risque d'être victime en sensibilisant les gens à propos des menaces de façon innovante et ludique. Cette recherche analyse la relation entre les facteurs individuels/situationnels et les perceptions d'être victime de *social engineering* au moyen d'un questionnaire. Le but final de cette recherche est d'obtenir un instrument efficace pour combattre les risques liés au *social engineering* en utilisant une méthode de sensibilisation par le *Serious Gaming* qui respecte les différences individuelles des participants.

## Management de la cyberdéfense

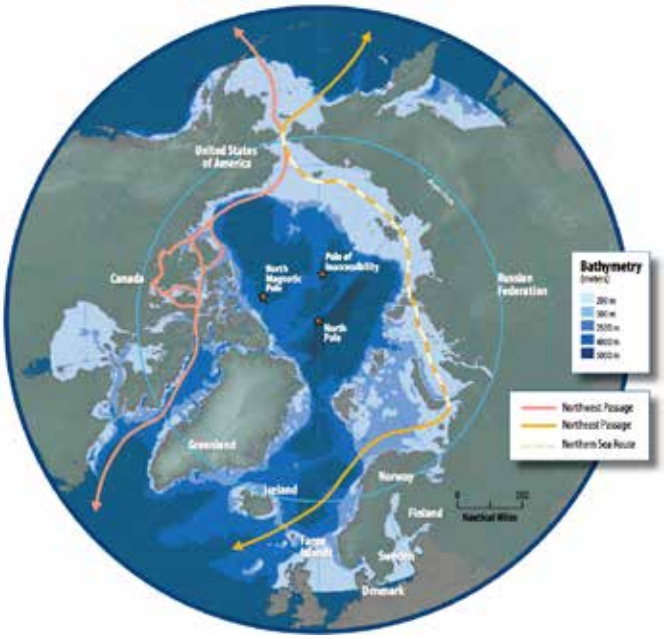
Deux projets de recherche consacrés au management de la cyberdéfense ont démarrés au début de l'année et devraient se terminer en 2023 par la publication d'un livre dédié à cette thématique. Comme dans les conflits conventionnels, l'armée doit d'abord être capable de se défendre dans le cyberespace avant de pouvoir remplir sa mission de défense nationale, de la population et des infrastructures critiques. La génération de cyber capacités, qui, à l'instar des services de renseignement, sont largement utilisées en temps de paix, diffère sensiblement de la génération de capacités militaires conventionnelles. Un problème de base commun, cependant, est que la puissance réelle requise est inconnue jusqu'à ce qu'un événement réel se produise. De plus, l'allocation de ressources financières ne suffit pas à elle seule à générer des prestations militaires.

5 https://serval.unil.ch/fr/notice/serval:BIB_5D54879D8F67

6 https://serval.unil.ch/fr/notice/serval:BIB_8A0DAC472C8F

7 https://www.springer.com/gp/book/9783030418250

8 L'éconophysique est un domaine de recherche scientifique qui propose de résoudre des problèmes économiques en appliquant des méthodes et des théories venant du domaine de la physique.




Carte de la région arctique montrant la route maritime du Nord, dans le contexte du passage du Nord-Est, et du passage du Nord-Ouest.

Le premier projet, chapeauté par Kilian Cuche, s'intéresse au management des ressources humaines pour la cyberdéfense et s'articule en trois parties. La première a pour but d'analyser les différents écosystèmes suisses impliqués dans la cyberdéfense (public, privé, et académique). La deuxième partie du projet s'intéresse aux capacités cyber et aura pour but de trouver des améliorations dans le transfert de connaissances et de compétences cyber entre ces trois écosystèmes. Finalement, la dernière partie sera consacrée à l'attractivité du secteur public, principalement l'armée, comme employeur cyber et aura pour but de donner des pistes pour améliorer le recrutement et la rétention du personnel dans le domaine cyber.

Le deuxième projet, réalisé par David Baschung, se penche sur les problématiques de gestion des ressources matérielles pour la cyberdéfense. Ce projet examine le processus global en ce qui concerne l'efficacité des capacités cyber de l'armée suisse. En effet, il ne suffit pas d'essayer uniquement d'optimiser le processus d'achat en termes de ressources matérielles cybernétiques, mais il faut plutôt avoir une vue globale du cycle, en commençant par la surveillance technologique, en passant par la planification des capacités, jusqu'à leur introduction dans le paysage des systèmes de production respectifs.

## L'impact des politiques économiques sur la sécurité

Les futurs travaux s'orienteront naturellement vers les thématiques liées à l'économie de la cyberdéfense mais aussi à des sujets purement d'ordre de l'économie militaire afin de continuer dans le domaine de recherche historique de la chaire. Par exemple, le prochain livre envisagé aura pour thématique les différents modèles de politiques économiques et leurs impacts sur la sécurité. Il permettra une comparaison des modèles totalement autarciques ou isolationnistes avec des modèles totalement mondialisés ou libertaires et analysera leurs conséquences sur la sécurité. Finalement, il tirera des conclusions sur ces modèles de politiques économiques et démontrera leurs avantages et inconvénients.

K. C.

### Sélection bibliographique

Keupp, MM. (2015) The Northern Sea Route: A Comprehensive Analysis. Wiesbaden: Springer Gabler. ISBN 978-3-658-04081-9

Keupp, MM. (2017) Der moderne Wirtschaftskrieg - Herausforderungen und Strategien : MILAK-Herbsttagung vom 10. September 2016. Militärakademie an der ETH Zürich Schriftenreihe. MILAK Schrift Nr. 17

Keupp, MM. (2019) Economie Militaire. Wiesbaden: Springer Gabler. ISBN 978-3-658-25287-8

Mermoud, A. (2019) Three Articles on the Behavioural Economics of Security Information Sharing: A Theoretical Framework, an Empirical Test, and Policy Recommendations. PhD Thesis. Université de Lausanne. Faculté des hautes études commerciales (HEC)

Percia David, D. (2020) Three Articles on the Economics of Information-Systems Defense Capability: Material-, Human-, and Knowledge-Resources Acquisition for Critical Infrastructures. PhD Thesis. Université de Lausanne. Faculté des hautes études commerciales (HEC)

Cuche, K. (2019) Guerre de l'information et politique: quelles conséquences pour la sécurité de la Suisse ? Revue Militaire Suisse, numéro 6, 2019.

Keupp, MM. (2020) The Security of Critical Infrastructures: Risk, Resilience and Defense. International Series in Operations Research & Management Science, Cham: Springer Nature. ISBN 978-3-030 41826-7

**ASIS International** (American society for industry security) est une association internationale rassemblant des professionnels de la sécurité et de la sûreté. Cette association a été créée en 1955 aux Etats-Unis.

*Economie de défense*

## ASIS International : La plus grande association au service des professionnels de la gestion de la sécurité

**Jean-Pierre Therre**
Vice-Chair ASIS Chapitre 160 – Switzerland.

Acteur incontesté depuis 1955 du développement et de l'avancement du secteur de la sécurité dans le monde, l'association professionnelle ASIS International (ci-après ASIS) s'est fixée pour mission de promouvoir l'excellence et le leadership au sein des professions de la sécurité.

Ainsi, en 2019, ASIS s'est engagé sur un nouveau plan stratégique s'appuyant sur quatre piliers structurés pour soutenir les professions de la sécurité au niveau mondial:

- Renforcer la reconnaissance des professions de la sécurité ;
- Elever la fonction sécuritaire pour influencer le succès organisationnel de l'entreprise ;
- Accélérer la transition digitale ;
- Servir les besoins globaux de notre société.

Et malgré l'impact des crises qui se succèdent dans le monde affectant durablement notre société et ses équilibres fondamentaux, ASIS ne cesse d'investir dans des programmes, des initiatives, des formations et des ressources pour répondre au mieux à la diversité des besoins de l'ensemble de ses membres, professionnels de la sécurité à tous les niveaux.

Historiquement orientée autour de la thématique de la sûreté et de la sécurité (y compris le renseignement et la gestion de crise), ASIS s'est beaucoup ouverte ses dernières années à la transversalité et à la convergence des différentes approches et techniques sécuritaires, en particulier en renforçant sensiblement son focus sur les thématiques touchant à la sécurité de l'information et à la résilience des entreprises.

### Structure et organisation de ASIS

Forte aujourd'hui de 34'000 membres (dont 10'300 certifiées) répartis dans 145 pays, ASIS compte 51 régions géographiques et 250 chapitres nationaux. Elle s'appuie également sur 34 communautés thématiques.

Ces communautés thématiques transversales permettent aux membres de réseauter, d'échanger leurs meilleures pratiques et de partager des solutions sécuritaires adaptées à leurs besoins spécifiques. Elles correspondent soit aux grands enjeux sécuritaires propres à chacun des grands secteurs économiques (banques et services financiers, agriculture et approvisionnements alimentaires, santé, industries pharmaceutiques, etc.), soit à des thématiques sociétales et professionnelles essentielles (résilience organisationnelle des entreprises, prévention des crimes, forces de sécurité publique, services privés de sécurité, gestion des risques humains, etc.).

La structuration et l'intrication de ses régions, de ses chapitres et de ses communautés thématiques ont été sensiblement renforcées pour favoriser la remontée diligente des informations et des préoccupations locales entre la base des membres et les comités centraux. Cette évolution se traduit par des propositions à valeur ajoutée propres à chaque région géographique, tenant compte des réalités locales et des composantes culturelles.

### Les grandes priorités de ASIS : la formation professionnelle et le développement de normes et standards

Bien entendu la formation continue et le développement professionnel de ses membres constituent pour ASIS une toute première priorité. Il s'agit de construire des cheminements clairs d'évolution de carrière et d'accompagner ou même d'accélérer le développement professionnel de ses membres le long de ces référentiels, lesquels visent un management de la sécurité par l'excellence, au niveau opérationnel, stratégique ou encore exécutif. Cette volonté s'exerce à travers de très nombreux programmes adaptés de formation continue, longs ou courts, régionaux ou internationaux, débouchant le plus


Cours ASIS dispensé en présentiel.

souvent sur l'obtention de certifications sécuritaires internationalement reconnues. Certaines de ces initiatives d'enseignement et de formation sont proposées dans le cadre de programmes de très hauts niveaux sous l'égide d'universités prestigieuses. A relever la possibilité offerte par la Fondation ASIS de bénéficier de bourse de soutien dans le cadre de projets de recherche pratique ou de formations académiques. Par exemple, construit sur le principe de l'exemplarité, le centre de leadership et de développement des CSOs (*Chief Security Officers*) est un forum exclusif de réseautage et de collaboration entre de hauts responsables de sécurité des grandes entreprises, lequel vise à souligner les évolutions des métiers de la sécurité, les attentes et les besoins correspondantes des professionnels.

Donc, que l'on soit à la recherche d'une nouvelle opportunité professionnelle ou que l'on soit un leader à la recherche des meilleurs talents pour ses équipe, ASIS cultive les compétences de ses membres et recense les opportunités. Ces opportunités sont très appréciées, en particulier pour ceux qui travaillent dans des environnements internationaux. Et par ailleurs son portefeuille de certifications professionnelles renforce les compétences de base et l'expertise.

Une autre orientation fondamentale de ASIS est l'élaboration puis la diffusion de normes, standards et recommandations visant à soutenir les professionnels dans leurs pratiques quotidiennes et dans leurs projets. Ces normes et standards sont publiées et mises à jour tout en tenant compte des obligations légales et règlementaires spécifiques aux régions et pays des membres. Ainsi, des représentants d'ASIS participent activement aux travaux des comités de normalisation, comme par exemple l'*ISO/TC 262 Risk Management* et l'*ISO/TC 292 Security and Resilience*.

**Favoriser la diffusion d'informations entre tous les professionnels de la sécurité**

Depuis de nombreuses années, ASIS s'applique à favoriser la transparence et l'inclusivité tout en tenant compte du caractère toujours plus « glo-cal » (global-local) de notre société.

Au sein même d'ASIS, la diffusion rapide, entre pairs, des informations, des questionnements et des réponses apportées est ainsi devenue une priorité. Cette diffusion est favorisée par différents portails de communications modernes, sécurisés et actualisés (*ASIS Connects*). En particulier, une plateforme virtuelle, dite *GSX+*, embarque pour quelques jours les différentes communautés, les réseaux et des entreprises partenaires dans un modèle collaboratif global d'échanges et de formation. Plus de 20'000 membres issus de 110+ pays (croissance de 15% chaque année) participent ainsi à plus de 150 sessions. Ces nombreux efforts d'information en ligne sont complétés par la publication plus classique d'une revue mensuelle *Security Management* qui, mois après mois, développe d'importantes thématiques d'actualités et souligne les orientations émergentes de la sécurité. Tout au long de l'année, des leaders d'opinion mondiaux, des CSOs et des experts de premier plan s'y expriment selon un calendrier de publications et d'apprentissages bien étudié.

Pour finir, une bibliothèque exceptionnelle permet de bénéficier d'avis compétents quant aux dernières et nombreuses publications sécuritaires disponibles (rapports de recherche, white papers, benchmarks).

**L'organisation européenne constitutive d'ASIS**

Avec 2'500 membres distribués dans 24 chapitres, la communauté d'ASIS est également devenue la plus grande association professionnelle du secteur de la sécurité en Europe.

Dans un monde « glo-cal », complexe et incertain, où même les petites-moyennes entreprises sont interconnectées et exposées comme les plus grandes, les menaces ne s'arrêtent pas aux frontières nationales. Et donc un réseau d'experts européens de la sécurité se doit d'être rapide, efficace et proactif au niveau continental. De fait, la présence européenne d'ASIS couvre presque

toutes les régions du continent européen et comprend aussi bien des représentants de grandes entreprises, leurs directeurs régionaux et leurs responsables fonctionnels, que des petits entrepreneurs, des conseillers et des innovateurs, tous spécialistes ou experts en matière de sécurité et de gestion des risques.

Ainsi les chapitres nationaux sont le cœur et l'âme même de la communauté européenne ASIS, créant aussi des opportunités de développement professionnel et de réseautage au niveau régional. A travers les réunions des sections locales ou encore lors de la conférence annuelle « ASIS Europe », l'évènement régional phare de l'association qui se tiendra du 31 mai au 2 juin 2021 à Prague, et au travers de *l'ASIS Connects*, ASIS offre à ses membres une portée inégalée pour le réseautage personnel et pour développer des collaborations actives. Ainsi, la conférence ASIS Europe constitue un rassemblement régional unique de leaders de la sécurité, bien établis et en herbe, de conseillers experts en matière de sécurité, de résilience et de gestion de crise. Un bulletin d'information régional mensuel intitulé *EuroDynamics* tient également les membres au courant des développements clés au sein d'ASIS ainsi que des faits saillants de l'actualité réglementaire de l'UE.

Cette communauté en ligne d'ASIS Europe permet donc aux membres de tout le continent de se connecter, de collaborer et de créer un réseau solide pour les professionnels européens de la sécurité. Ces membres peuvent oser des questions, partager leurs expériences et rester informés, notamment quant aux problématiques systémiques transrégionales ou transfrontalières.

De la formation locale ou régionale des cadres aux échanges collaboratifs mondiaux, un solide calendrier d'événements est conçu pour soutenir la croissance professionnelle et faire progresser la carrière de tous.

**Le chapitre suisse « ASIS 160 Switzerland »**

Le chapitre suisse dit *Chapter 160 Switzerland* a été fondé en 1983 et compte actuellement une petite centaine de membres. Toutefois, à l'occasion de ses différents évènements annuels, il s'adresse à plus de 300 invités - des professionnels de la sécurité de tous types d'entreprises et/ou des institutions fédérales / cantonales. Il répond à un large éventail de secteurs et besoins de la profession de sécurité en Suisse. La stabilité sociale et économique traditionnelle de la Suisse favorise en effet une grande diversité d'activités commerciales.

Divisé en deux régions, le chapitre suisse organise successivement des événements éducatifs et de réseautage, des conférences et des ateliers en Suisse alémanique et en Suisse romande. Du fait de sa relative modestie, il entretient des liens forts avec des sections des pays voisins, en particulier, pour promouvoir des événements éducatifs et de partage d'informations.

Dans le cadre de sa mission de promotion du réseautage professionnel et de la formation, le chapitre suisse d'ASIS

Cours ASIS dispensé sous forme de webinar.

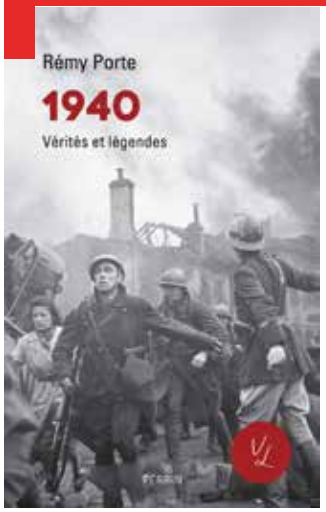
s'attache à organiser chaque année une demi-douzaine d'événements au bénéfice de ses membres et de ses partenaires institutionnels ou privés. Les thématiques ainsi abordées en 2019 et 2020 concernaient aussi bien la sécurisation complexe des chaines logistiques d'approvisionnements (Amazon), les conditions d'organisation et de gestion de la résilience/continuité de grandes entreprises internationales (Lafarge Holcim) mais aussi les processus de décision et de conduite entre la Confédération et Cantons à l'occasion de la crise pandémique actuelle (Intervention A. Vautravers). Le chapitre encourage encore activement ses membres à participer à des évènements thématiques (séminaires, conférences, etc.) orchestrés par ses partenaires institutionnels (GCSP, CSS-ETHZ, etc.), privés (SOS International, Securitas, Etic Sa, Risk In) ou académiques. En particulier le chapitre suisse, référence et promeut des programmes de formation continue (CAS, DAS, MAS) développés par les universités et hautes écoles suisses. Pour finir, le chapitre met en œuvre en Suisse des initiatives internationales favorisant l'inclusion comme le forum « Women in Security » ou l'initiative « Young Professional Award ». Ce dernier est destiné à soutenir de très jeunes professionnels de la sécurité et à valoriser les projets innovants qu'ils auraient développés.

A travers ces différentes initiatives, le chapitre suisse d'ASIS s'applique à renforcer sa mission fédératrice au bénéfice des professionnels de la sécurité issus de tous les secteurs institutionnels ou économique et souhaite favoriser un rapprochement conforme à un vieux principe libéral suisse : l'unité, par l'éthique et les pratiques, dans la diversité, des cultures, des expériences et des analyses.

J-P. T.

**Pour tout contact :**

www.asisonline.ch
www.asisonline.org
Etienne Ammon : chairman@asisonline.ch
Jean-Pierre Therre : vc-west@asisonline.ch





La question occupe les historiens suisses et étrangers depuis la fin du service actif en août 1945. Les réponses varient en fonction des périodes et des contextes, certains affirmant même que notre pays n'a jamais été réellement menacé par une agression armée. Ce livre entend montrer que cette question n'a rien de farfelu et qu'une réponse sérieuse, sous la forme d'une uchronie ou, si l'on utilise un anglicisme, d'une histoire alternative, peut lui être donnée sans sombrer dans le roman tragique.

*Recension*

## 1940-2020 : Deux années clé

**Rédaction RMS+**

A l'occasion de la commémoration de la campagne de France de 1940, plusieurs livres ont été publiés, parmi lesquels un *1940. Vérités et légendes* du colonel Rémy Porte et un *Et si la Suisse avait été envahie ? 1939-1945* des colonels Hervé de Weck et Pierre Streit.

En 30 chapitres, le colonel Porte revient sur ce chapitre funeste de l'histoire militaire française, en répondant en quelques pages et de manière précise à une série de questions clé : le commandement français était-il à la hauteur ? Fallait-il déclarer Paris ville ouverte ? La ligne Maginot était-elle une bonne idée ? Même s'il ne contient aucune nouvelle révélation sur un événement qui a déjà fait l'objet de nombreuses études, l'ouvrage du colonel Porte remet cette « étrange défaite » (Marc Bloch) en perspective, en montrant par exemple que la France porte en réalité seule le poids de la bataille terrestre, avec une centaine de divisions, alors que le corps expéditionnaire britannique se réduit à une dizaine et qu'il n'est pas prêt à livrer bataille. Cette situation rappelle « étrangement » les propos récents de l'ancien chef de l'Etat-major général de l'armée britannique, le général Sir Mike Jackson : « *Nous sommes dans la position où vraiment, si nous faisons les choses correctement, nous pouvons aligner une seule division. Peut-être de deux ou trois brigades. C'est l'effort maximal que nous pourrions attendre de l'armée d'aujourd'hui* » (*Daily Mail*, 8 août 2020).

Une autre question est traitée : qu'en a-t-il été du soldat français, de sa combativité ? Est-ce que Céline avait tort ou raison lorsqu'il résume ainsi la période qui va de septembre 1939 à l'attaque allemande du 10 mai 1940 : « *Neuf mois de belotte, six semaines de course à pied* » ? Comme le bilan des pertes le montre bien (de l'ordre de 50-60'000 soldats français tués en près de 50 jours de combats), le soldat français s'est battu, souvent avec ténacité, chaque fois qu'il a été en mesure de le faire, c'est-à-dire qu'il a été commandé. Au-delà des matériels et des erreurs de conception, la défaite de 1940 est donc avant tout une défaite d'ordre intellectuel, ce que d'autres auteurs avaient déjà mis en évidence, en particulier l'historien suisse Ladislas Mysyrowicz (*Autopsie d'une défaite : origines de l'effondrement militaire français de 1940*, Lausanne, Editions L'Age d'homme, 1973). Comme le souligne le colonel Porte (p. 160), l'état-major français postule de manière erronée que son homologue allemand va se battre comme lui.

On ne peut que recommander également la lecture de *L'Etrange défaite* de l'historien Marc Bloch, du *Drame de 1940* du général Beaufre, réédité en 2020, ou encore de *L'étrange capture*, le récit du colonel Montjean. Pierre Montjean, officier d'état-major de la 1ère Armée et chef de la section « Opérations » du 3ème Bureau, est capturé par les Allemands à Steenwerck, le 29 mai 1940. Lors des premiers jours de sa captivité, il retrace, encore sous le choc, l'enchaînement dramatique des événements. Le récit qu'il fait de ces vingt jours qui auront précédé son « étrange capture » constitue un témoignage unique puisque les archives de la 1ère Armée ont été brûlées.

Dans leur ouvrage qui se veut une uchronie et pas un roman-fiction, Hervé de Weck et Pierre Streit reviennent de leur côté sur une question qui, quoi qu'on en dise, reste controversée : pourquoi la Suisse n'a-t-elle pas été envahie en 1940 ou plus tard ? De fait, la question occupe les historiens suisses et étrangers depuis la fin du service actif en août 1945. Les réponses varient en fonction des périodes et des contextes, certains affirmant même que la Suisse n'a jamais été réellement menacée par une agression armée, parce qu'elle a notamment coopéré économiquement avec l'Allemagne, son principal partenaire économique d'alors et encore de nos jours d'ailleurs.[1]

1 Voir le récent article d'Hans Ulrich Jost, *So kooperierte die Schweiz mit Hitler-Deutschland*: https://www.infosperber.ch/Politik/Schweiz-Nazi-Deutschland-Handelsvertrag-1940 (lien actuel)

Entre la légende dorée (celle de la Suisse résistante) et la légende noire (la Suisse complice du nazisme), une histoire globale de la Suisse pendant la Seconde Guerre mondiale reste à écrire, afin qu'elle prenne en particulier en compte la dimension du renseignement ou celle de la menace réelle ou perçue comme tel.

Le livre entend montrer que cette thématique reste pertinente et qu'une réponse sérieuse, sous la forme d'une uchronie ou l'examen des possibles, peut lui être donnée sans sombrer dans le roman fiction. Ce d'autant plus qu'à certains moments de la Seconde Guerre mondiale, le service de renseignement suisse, en général perspicace et bien informé, a mal apprécié et interprété les intentions de l'Axe, ce qui a faussé sa vision de la menace réelle qui planait alors sur notre pays. Mi-mai 1940, il voit une invasion imminente à laquelle le commandement de la Wehrmacht ne pense pas. La menace, telle que la perçoivent le SR, les autorités politiques et militaires ou encore la population, ne correspond ainsi pas forcément à la menace réelle. C'est le « brouillard de la guerre » et c'est à partir de celui-ci que les auteurs se risquent à se demander : « Et si la Suisse avait été envahie ? »

Il serait hasardeux de tirer des parallèles entre 1940 et 2020, mais force est de constater que, dans les deux cas, la situation internationale est marquée par l'incertitude. A l'été 1940, l'Allemagne victorieuse est encore libre de ses choix stratégiques. Elle peut se tourner vers le bassin méditerranéen afin d'étrangler l'Empire britannique et le pousser à la paix. En 2020, la crise sanitaire, le dérèglement climatique et le retour de la politique de puissance sous toutes ses formes rendent toute prévision bien aléatoire. Si le principe de Thiers « gouverner, c'est prévoir » n'est pas oublié, il ne faut donc pas baisser la garde.

*News*

**Révision de la loi sur le renseignement : nouvelles décisions du Conseil fédéral**

Berne, 26.08.2020 – La loi sur le service de renseignement est actuellement en cours de révision. En l'occurrence, il s'agit aussi de prendre en compte les exigences formulées par la DélCdG concernant le traitement des données – comme une simplification de l'environnement système. De plus, il y a lieu d'intégrer aux travaux de révision les constatations de l'autorité de surveillance indépendante AS-Rens. C'est pourquoi le Conseil fédéral, lors de sa séance du 26 août 2020, a prolongé jusqu'à fin 2021 le mandat du DDPS, chargé d'établir un projet de consultation. Les aspects prévus jusqu'ici dans le cadre de la révision resteront maintenus dans la suite des travaux.

La loi sur le renseignement (LRens) est en vigueur depuis le 1er septembre 2017. Avant cette date, le Conseil fédéral avait déjà envisagé de régler certains points en suspens dans le cadre d'une révision. Début 2019, le Conseil fédéral a donc chargé le DDPS d'établir un projet de consultation d'ici la fin de l'été 2020.

**Simplification de l'environnement système**

Le Conseil fédéral a maintenant décidé de prolonger le mandat du DDPS jusqu'à la fin 2021. Il sera ainsi possible de prendre en compte dans la révision les exigences relatives au traitement des données que la Délégation des commissions de gestion (DélCdG) a formulées dans son rapport d'activité 2019. Il s'agit notamment de simplifier l'environnement système, ce qui exige l'introduction de nouveaux concepts et règlementations dans le chapitre « Traitement des données et archivage ». La suite des travaux permettra d'exposer en détail comment cette simplification se concrétisera.

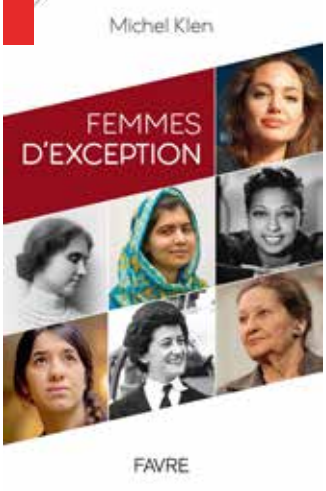
La révision prendra aussi en considération une expertise de l'Office fédéral de la justice soulignant les différences d'interprétation juridique que peuvent parfois avoir la DélCdG et le Service de renseignement de la Confédération pour ce qui est des restrictions de traitement des données définies à l'art. 5, al. 5 et 6, LRens. Elle intégrera aussi les résultats des examens menés par l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens).

**Examen des modifications relatives aux mesures de recherche d'informations**

Les autres aspects de la révision restent inchangés. Outre des corrections d'ordre formel, la révision a pour but d'examiner si des mesures de recherche soumises à autorisation sont également nécessaires dans le domaine de l'extrémisme violent. Actuellement, il est exclu de surveiller la correspondance par poste ou par télécommunication ou encore de s'introduire dans des systèmes ou des réseaux informatiques en vue d'obtenir des informations sur des extrémistes violents ; cela en regard du principe de proportionnalité et de la proximité des groupes extrémistes violents avec des mouvements idéologiques et politiques. L'extrémisme violent ayant toutefois pris de l'importance en tant que forme de menace pour la sécurité intérieure et extérieure de la Suisse, on examine actuellement comment adapter les possibilités d'acquérir des informations en cas de menace majeure.

De plus, la révision prévoit de confier intégralement à l'AS-Rens les tâches de l'actuel Organe indépendant de contrôle pour l'exploration radio et l'exploration du réseau câblé.

Source : https://www.vbs.admin.ch/content/vbs-internet/fr/ueber-das-vbs/organisation-des-vbs/die-verwaltungseinheiten-des-vbs/-der-nachrichtendienst-des-bundes.detail.nsb.html/80177.html




Toutes les photos © Auteur.

*International*

## Des femmes dans la guerre

**Michel KLEN**
Département de la sécurité, de l'emploi et de la santé (DSES). Police Internationale – Section Migration

Le livre *Femmes d'exception* qui vient d'être publié aux éditions Favre nous rappelle le rôle important, souvent mal connu, que les combattantes ont joué dans les guerres. Beaucoup, célèbres ou anonymes, ont fait preuve de bravoure et d'abnégation dans des situations critiques. Cette saga poignante comporte notamment les agents de renseignement, les infirmières, les ambulancières, les résistantes qui se sont engagées dans les deux guerres mondiales. Dans les douloureux conflits dans lesquels la France a été mêlée en Indochine puis en Algérie, la plupart sont restées oubliées telles les prostituées à Dien Bien Phu devenues des soignantes héroïques dans l'enfer pathétique de la cuvette indochinoise transformée en véritable mouroir, les plieuses de parachutes travaillant sans relâche jour et nuit sous des températures extrêmes et les IPSA (infirmières parachutistes secouristes de l'air) qui ont sauvé de nombreuses vies humaines lors de missions périlleuses. Cet article se limitera toutefois aux guerrières qui ont pris les armes pour sauver leur communauté en danger. Dans ce registre, les exemples des chrétiennes du Liban et des *peshmergas* kurdes sont révélateurs des possibilités extraordinaires de ces filles de Vénus plongées dans la tourmente de Mars, le dieu impitoyable de la guerre.

### Les chrétiennes du Liban

La guerre civile qui a déchiré le pays du cèdre entre 1975 et 1990 a été marquée par des combats sanglants entre les groupes religieux, les familles et les chefferies féodales par milices interposées, en particulier entre phalangistes chrétiens et *fedayins* palestiniens. Dans ce théâtre d'affrontements meurtriers, des femmes ont accompli des actes d'héroïsme. Parmi celles-ci, Jocelyne Khoueiry, une chrétienne maronite qui s'est surpassée pour défendre sa communauté menacée de disparition. Lorsque la tragédie éclate en avril 1975, la jeune Libanaise n'a pas encore 20 ans. Transcendée par sa fougue juvénile et un patriotisme ardent, elle sera l'une des rares combattantes à lutter avec des commandos d'élite, à diriger des unités féminines et à s'imposer comme véritable chef de guerre, un comportement qui lui vaudra le surnom élogieux de *Raïsseh* (féminin de chef en arabe). Pour parfaire sa formation militaire, en particulier au combat de rue, Jocelyne s'entraîne avec d'autres filles très motivées au camp de Qamaz. Dans l'encadrement se trouve Francis Borella, un ancien officier de la Légion étrangère qui fournit de précieux conseils aux jeunes guerrières. Mais le légionnaire expérimenté sera tué quelques semaines plus tard lors d'un affrontement avec des Palestiniens. Son instruction terminée, la jeune femme se battra avec d'autres militantes. Dans la nuit du 6 au 7 mai 1976, elle devient une héroïne en remportant avec six autres adolescentes une victoire éclatante contre une centaine de commandos palestiniens. Encerclées dans un immeuble de Beyrouth, les femmes soldats Laure, Brigitte, Gisèle, Dolly, Marcelle et la petite Nina (14 ans), galvanisées par une Jocelyne survoltée, réussissent à surprendre leurs adversaires déchaînés et à retourner une situation qui semblait compromise. Ses biographes ont raconté cette bouleversante séquence de combat :

« *Il est 22 heures. Une roquette et des grenades explosent, des salves de mitrailleuses déchiquettent les murs du bâtiment dans un fracas assourdissant. L'immeuble tremble, les plâtres s'effondrent, [...]. Jocelyne n'y croit plus trop, mais n'en fait rien savoir : sous son impulsion et ses ordres, elles (les combattantes) continuent le combat. Tout semble perdu, mais Jocelyne risque une ultime manœuvre. Elle remonte sur la terrasse, prenant bien garde de ne pas se faire repérer. Sautant d'un toit d'immeuble à l'autre – ils sont tous contigus – elle parvient à contourner ses adversaires. Elle tente de retenir son souffle qui s'est fait haletant [...]. Une dernière respiration et elle jette ses grenades en s'appliquant le plus possible, se baisse à toute vitesse pour se relever aussitôt et vider le chargeur de sa mitraillette. En bas, la panique se fait entendre. Leur chef a été tué et ils se replient en criant.* »[1]

1 Nathalie Duplan et Valérie Raulin, *Jocelyne Khoueiry, l'indomptable,* ed. Le Passeur, 2015.

Cette nuit-là, Jocelyne Khoueiry est devenue une figure légendaire à la tête de sa mini-armée entièrement féminine. L'exploit incroyable de la *Raïsseh* a été relaté dans la presse locale. Il a stimulé d'autres combattantes qui se sont engagées dans des milices au service de leur patrie. A l'instar de cette femme d'exception, d'autres chrétiennes du Liban ont fait preuve de bravoure, mais pour la plupart, leurs actes sont restés dans l'ombre de l'actualité.

**Les guerrières kurdes contre Daech**

Pour lutter contre les djihadistes de *Daech,* les femmes soldats comptent beaucoup sur l'extraordinaire ascendant psychologique qu'elles possèdent sur les fous de Dieu. Ces derniers étaient en effet terrifiés d'être tués par une femme. La propagande islamiste martèle qu'un djihadiste abattu par une combattante devient un « faux martyr » et ne peut donc entrer au paradis. De ce fait, il se voit privé de rapports sexuels illimités avec les vierges qui attendent les « vrais martyrs » dans l'espace céleste censé procuré la béatitude éternelle après la mort.

Dans la bataille contre *Daech,* les combattantes kurdes ont mené des actions méritoires. Elles ont été enrôlées dans les *peshmergas,* un terme qui qualifie les guerriers du Kurdistan. Le mot signifiant « au-devant de la mort » souligne parfaitement l'attitude du soldat qui se battra jusqu'à trépas. Aujourd'hui, il y aurait environ vingt mille femmes kurdes servant dans les forces du Kurdistan. Leur engagement dans la bataille de Kobane (au nord de la Syrie à proximité de la frontière turque) entre novembre 2014 et juin 2015 a été l'une des clés du sauvetage de la ville face à l'agression des djihadistes.

La combativité des femmes kurdes est due à l'état d'esprit martial qui leur est inculqué dès le plus jeune âge. Cette éducation est la résultante d'une histoire mouvementée. Le Kurdistan n'a jamais constitué une entité politique unifiée. Actuellement, son espace géographique s'étend sur plusieurs pays (Arménie, Turquie, Syrie, Irak, Iran) et alimente des foyers de contestation durables. Dans ce contexte belliqueux, la notion de défense de leur identité constitue une valeur sacrée. Les femmes sont partie prenante de ce concept d'autodéfense armée. C'est ainsi qu'ont été mis sur pied dans les villes des groupes de protection composés uniquement de femmes, les YPS-Jin (unités de défense civile), et des unités de combattantes au sein des guérillas, les YJA-Star. Dans ces sections de commandos, les jeunes femmes ne reçoivent pas seulement une formation militaire, mais elles apprennent à vivre sur le terrain en communauté dans les montagnes.

La libération de Raqqa au centre de la Syrie, capitale du califat autoproclamé de *Daech,* en octobre 2017, a mis en lumière les guerrières kurdes, en particulier l'une de ses leaders, Rodja Felat. Cette Syrienne de 36 ans était à la tête de trente mille combattants kurdes et arabes appartenant aux Forces démocratiques syriennes (FDS) dans l'opération « colère de l'Euphrate » qui a permis la reconquête de la ville tombée aux mains des islamistes trois ans plus tôt. L'action des FDS était appuyée par les forces spéciales américaines, britanniques et françaises. Rodja Felat est un pur produit du féminisme en armes qui a réussi à

La conférence de presse organisée pour annoncer la tenue de l'exercice cadre d'état-major ERNS 19.

diriger une armée pour faire tomber l'un des bastions terroristes au Proche-Orient. Cette jeune commandante de petite taille, mais avec un cœur gros comme çà, se déplace toujours avec sa garde rapprochée, deux jeunes femmes d'une vingtaine d'années, animées comme elle par un patriotisme sans faille et un esprit d'abnégation. A des journalistes qui l'interrogeaient, elle a confié que son héros préféré était Napoléon dont elle admire les qualités de stratège au service d'une ambition pour la grandeur de son peuple. Le clin d'œil avec la problématique kurde est prégnant.

Pour combattre *Daech,*les femmes kurdes utilisent aussi l'arme redoutable de la communication. Dans ce registre, c'est la chanteuse populaire Helly Luv qui porte le flambeau de la lutte en produisant des clips dans lesquels elle appelle à défendre le Kurdistan contre ses ennemis. Le plus célèbre, *Révolution,* paru en 2015, a eu un effet mobilisateur. L'artiste guerrière y apparaît en tenue de combat, cheveux rouge sang, portant autour de la taille et du cou des bandes de munition de mitrailleuse. Elle arrête à elle seule une colonne de chars en brandissant un panneau *Stop the violence* puis montre un drapeau kurde aux agresseurs. La scène est accompagnée d'une musique envoûtante et de paroles martiales qui renforcent la puissance du message. Lorsqu'elle a été filmée en train de chanter et de danser, la diva combattante n'était qu'à trois kilomètres des djihadistes de *Daech* dans une zone frontalière entre la Syrie et la Turquie où avait lieu de véritables bombardements et où on apercevait des habitants apeurés fuyant les tueurs islamistes. C'est précisément la mise dans une ambiance surréaliste et gravissime qui a fait de ce document bouleversant un événement exceptionnel.

Comme les chrétiennes du Liban, les combattantes kurdes ont bravé les préjugés en démontrant sur les théâtres de guerre qu'elles étaient capables de se dépasser. La fonction grandissante des femmes dans la chose militaire en général, les opérations à hauts risques en particulier, constitue l'un des faits de société de notre époque. Il y a plus d'un siècle, George Sand, l'une des fortes personnalités de la littérature française, nous avait prévenu : « *Une femme quand elle est héroïque, ne l'est pas à demi.* » (*Elle et lui,* 1859).

M. K.

# PLUS HAUT.
# PLUS VITE.
# PLUS SÛR.
# SUPÉRIORITÉ AÉRIENNE ET SOUVERAINETÉ DES DONNÉES.

WE MAKE IT FLY

L'Eurofighter est l'avion privilégié des forces aériennes européennes. Conçu par quatre nations partenaires, il assure indépendance et autonomie. Les excellentes performances de l'Eurofighter offriront une protection éprouvée à la Suisse. Il garantira son indépendance opérationnelle et la souveraineté de ses données.

Sécurité. Autonomie. We make it fly.*

*Nous faisons voler.

airbus.com
eurofighter.ch

AIRBUS