ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité » n°65
Lundi 22 janvier 2024

État stratège et cybersécurité

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 1 Cybersécurité et E-santé

Table des matières

Introduction

La conférence, intitulée « **État stratège et Cybersécurité** », organisée dans le cadre des "**Lundi de la Cybersécurité**", animée par **Bernard Besson**, président du comité scientifique de la Commission intelligence économique des Ingénieurs et Scientifiques de France (IESF), s'est tenue pour aborder un sujet d'importance capitale dans notre ère numérique. Cette session, menée par Bernard Besson, ex haut fonctionnaire du ministère de l'Intérieur, a offert une plateforme pour discuter du rôle vital de l'État dans la protection de la cybersécurité et la garantie de la liberté des citoyens dans un environnement numérique complexe.

Objectif de la Conférence :

L'objectif principal de cette conférence était de mettre en lumière l'importance stratégique de l'État dans le domaine de la cybersécurité. Elle visait à explorer comment un État démocratique, tout en préservant la liberté d'action et d'expression de ses citoyens, peut efficacement contrer les cybermenaces croissantes dans un monde ultra-connecté. La conférence s'est concentrée sur la nécessité pour l'État d'adopter une stratégie proactive et éclairée pour protéger non seulement ses infrastructures informationnelles mais également ses citoyens, soulignant le rôle crucial de la sensibilisation, de l'éducation et de la collaboration entre les secteurs public et privé.

Contexte et Intervenants :

Dans un contexte mondial où les cyberattaques et les menaces visant la sécurité des données deviennent de plus en plus sophistiquées et fréquentes, cette conférence a mis en exergue le rôle de l'État en tant que stratège dans la lutte contre ces menaces. Bernard Besson, aujourd'hui président de la société BBCyber, contrôleur général honoraire de la police nationale et auteur de nombreux romans passionnants sur la cyberdéfense, avec son expertise reconnue dans le domaine de l'intelligence économique et son expérience au ministère de l'Intérieur, a apporté une perspective unique sur les interrelations entre cybersécurité, politique et stratégie d'État.

La conférence a également souligné l'importance des initiatives telles que la plateforme **cybermalveillance.gouv.fr** et l'**ANSSI**, illustrant comment l'État peut soutenir les individus et les organisations face aux cybermenaces. L'accent a été mis sur l'évolution de la cryptologie et son rôle central dans la stratégie de l'État, en particulier dans des périodes de conflits et de tensions géopolitiques, comme l'a illustré la mise en place du système de messagerie instantanée chiffrée **Olvid**.

Cette conférence a ainsi offert une perspective complète et actuelle sur le rôle de l'État dans la préservation de la sécurité numérique, en mettant en avant les défis, les opportunités et les responsabilités partagées dans la bataille contre les cybermenaces. La contribution de Bernard Besson, avec son approche pédagogique et son expertise approfondie, a permis de mieux comprendre comment les stratégies d'État et la cybersécurité doivent collaborer pour anticiper et contrer les menaces numériques émergentes.

I. Le rôle de l'État stratège dans la Cybersécurité

Dans la première partie de sa conférence, Bernard Besson a abordé de manière approfondie le rôle de l'État en tant que stratège dans le domaine de la cybersécurité. Il a souligné que la responsabilité première de l'État est de garantir la sécurité de ses citoyens, notamment face aux menaces croissantes dans le cyberespace. Bernard Besson a mis en lumière plusieurs initiatives et structures clés mises en place par l'État français pour lutter contre les cybermenaces.

Tout d'abord, Monsieur Besson a présenté la plateforme cybermalveillance.gouv.fr comme un exemple de l'engagement de l'État dans la lutte contre les cyberattaques. Cette plateforme, créée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), sert de point de contact pour les particuliers et les entreprises victimes de cyberattaques. Elle offre des conseils et met en relation ceux qui demandent de l'aide avec des experts en cybersécurité. L'ANSSI, en tant qu'organisme interministériel, dépendant du Premier ministre, joue un rôle central dans la stratégie nationale de cybersécurité. Monsieur Besson a souligné son importance dans l'élaboration de politiques et de mesures de protection contre les menaces numériques.

Ensuite, le conférencier souligne l'importance des compétences humaines et de la confiance organisationnelle. En effet, au-delà des aspects technologiques, M. Besson a insisté sur l'importance des compétences humaines dans la cybersécurité. Il a fait valoir que la formation, la sensibilisation et la fidélisation des personnels sont essentielles pour maintenir un niveau élevé de sécurité informatique. La confiance organisationnelle a été présentée comme un élément crucial. Selon M. Besson, les défaillances humaines, souvent dues à un manque de confiance ou de sensibilisation, peuvent être aussi préjudiciables que les faiblesses technologiques. Il a donc encouragé les organisations à développer une culture de sécurité robuste.

Enfin, l'expert a mis en avant que la stratégie de l'État ne se limite pas à la réponse aux incidents, mais inclut également une dimension préventive et éducative. La sensibilisation du grand public et la formation des acteurs du secteur privé et public sont des composantes essentielles de cette stratégie. L'État doit aussi anticiper les évolutions futures en matière de cybersécurité et adapter en continu ses stratégies pour faire face aux nouvelles menaces.

En conclusion de cette première partie, M. Besson a réaffirmé que l'État, en tant que stratège, doit adopter une approche globale pour la cybersécurité, impliquant non seulement des mesures technologiques avancées mais aussi un investissement dans le capital humain et la construction d'une culture organisationnelle forte autour de la sécurité numérique.

II. Les défis de la Cybersécurité dans un contexte de conflit

Dans la deuxième partie de sa conférence, Bernard Besson a exploré les défis spécifiques de la cybersécurité dans un contexte de conflit mondial. Il a utilisé l'exemple des Jeux Olympiques pour illustrer comment les événements d'envergure mondiale peuvent devenir des cibles de cyberattaques, mettant en évidence la nécessité d'une collaboration étroite entre les institutions étatiques et les acteurs privés.

Premièrement, le spécialiste a choisi les Jeux Olympiques comme un exemple concret pour montrer comment un événement international peut se transformer en un "champ de bataille" pour la cybersécurité. Il a souligné que, dans le contexte actuel de tensions géopolitiques, des événements tels que les Jeux Olympiques ne sont pas seulement des célébrations sportives, mais aussi des cibles potentielles pour divers types de cyberattaques. L'événement sert de plateforme pour démontrer comment les États, tout en cherchant à protéger leurs infrastructures et leurs citoyens, doivent également sécuriser des événements d'importance internationale.

Bernard besson a insisté sur la nécessité d'une collaboration étroite entre l'État et les entreprises privées, en particulier celles impliquées dans la technologie et la cybersécurité. Il a mentionné des entreprises comme Atos, Cisco et Orange, qui jouent un rôle clé dans la sécurisation d'événements d'une telle ampleur. Cette coopération est essentielle pour partager les connaissances, les technologies et les ressources afin de construire une défense robuste contre les cybermenaces. Il a souligné que l'expertise technique du secteur privé, combinée aux capacités et à l'autorité de l'État, crée un cadre de cybersécurité plus efficace.

La conférence a abordé la dimension politique de la cybersécurité dans les contextes de conflit. M. Besson a évoqué des décisions politiques, comme l'éviction d'Alibaba, un partenaire chinois initialement envisagé pour les Jeux Olympiques, soulignant comment la cybersécurité peut être influencée par des considérations géopolitiques. Il a également discuté de la manière dont les cyberattaques lors d'événements mondiaux peuvent avoir des répercussions politiques et stratégiques importantes, influençant les relations internationales et la perception publique.

Enfin, l'intervenant a abordé les défis humains et organisationnels dans la cybersécurité en temps de conflit. Il a évoqué la rotation des personnels, la formation et le maintien des compétences en cybersécurité comme des éléments cruciaux pour une stratégie de défense efficace. Il a souligné que la gestion des ressources humaines en cybersécurité n'est pas seulement une question de recrutement, mais aussi de rétention des compétences et de développement de la confiance au sein des organisations.

En résumé, cette partie de la conférence a mis en évidence que dans un contexte de conflit mondial, les défis de la cybersécurité ne sont pas uniquement technologiques, mais impliquent également des considérations politiques, stratégiques et humaines. M. Besson a souligné l'importance de la collaboration entre les secteurs public et privé, ainsi que la nécessité d'une planification et d'une préparation minutieuses pour faire face aux cybermenaces dans des situations de conflit.

III. La Cybermenace interne et externe

Dans la troisième partie de sa conférence, Bernard Besson a abordé la complexité des cybermenaces, soulignant que les défis en matière de cybersécurité viennent tant de l'extérieur que de l'intérieur des organisations.

L'expert a souligné l'importance pour un État stratège de reconnaître que les cybermenaces ne proviennent pas uniquement de sources externes, mais peuvent aussi émaner de l'intérieur. Il a abordé la difficulté de déterminer l'emplacement et l'identité de l'adversaire dans le domaine de la cybersécurité. Il a expliqué que, souvent, les menaces internes sont négligées ou sous-estimées. Ces menaces peuvent inclure des défaillances humaines, des erreurs, ou même des actes malveillants de la part des employés.

Par ailleurs, Bernard Besson a fait valoir que les problèmes de cybersécurité ne sont pas toujours dus à des failles technologiques, mais sont souvent exacerbés par des défaillances humaines. Il a mentionné l'absence de confiance au sein des organisations comme une faiblesse majeure. Il a souligné que ces problèmes humains ont des implications quasi-philosophiques, affectant le quotidien de la cybersécurité. Les organisations doivent prendre en compte ces aspects humains pour renforcer efficacement leur sécurité numérique.

Le discours de M. Besson a également abordé l'importance de la gestion des ressources humaines dans la cybersécurité. Il a souligné que la rotation du personnel et la perte de savoir-faire en matière de cybersécurité constituent un défi majeur pour les organisations. Il a mentionné que la politique de cybersécurité doit également être une politique de gestion des ressources humaines, impliquant la formation continue du personnel et la préservation des compétences en cybersécurité au sein de l'organisation.

L'intervenant a élargi la discussion pour inclure des considérations philosophiques et organisationnelles dans la stratégie de cybersécurité. Il a abordé la manière dont les problèmes de confiance et les défaillances humaines s'imbriquent dans les défis quotidiens de la cybersécurité. Il a encouragé les organisations à envisager des améliorations et à envisager des stratégies qui tiennent compte des aspects humains et organisationnels de la cybersécurité.

En résumé, dans cette partie de la conférence, Bernard Besson a mis en lumière la complexité des menaces en cybersécurité, en soulignant que **les dangers ne viennent pas seulement de l'extérieur, mais aussi de l'intérieur des organisations**. Il a insisté sur l'importance de la gestion des ressources humaines et de la confiance organisationnelle dans le cadre d'une stratégie de cybersécurité efficace.

IV. L'importance des renseignements humains dans la Cybersécurité

Dans la quatrième partie de sa conférence, Bernard Besson a mis l'accent sur le rôle crucial du renseignement humain (**HUMINT**) dans la stratégie globale de cybersécurité.

Le professionnel a commencé par souligner l'importance de la complémentarité entre le renseignement d'origine électromagnétique (**SIGINT**) et le renseignement humain. Il a expliqué que, bien que le SIGINT soit essentiel dans le monde moderne pour la collecte d'informations automatisée, il ne peut remplacer la richesse et la profondeur des insights fournis par le

HUMINT. Il a illustré cela en faisant référence à des situations réelles où des défaillances dans le renseignement humain ont conduit à des interprétations erronées des données ou à des réactions inadéquates aux menaces.

M. Besson a abordé la complexité de la gestion des sources humaines, en soulignant qu'elle implique des risques et nécessite une implication significative. Le recrutement et la gestion des informateurs, selon lui, requièrent un haut degré de prudence, de compétence et d'engagement. Il a souligné que le travail avec les sources humaines est un effort continu, nécessitant une vigilance 24 heures sur 24, contrairement à certains aspects du SIGINT qui peuvent fonctionner de manière plus automatisée.

Pour illustrer ses propos, l'intervenant a cité des exemples historiques et contemporains où le renseignement humain a joué un rôle crucial. Il a notamment parlé de la crise des missiles de Cuba en 1962 comme d'un cas où la compréhension des intentions et des pensées des dirigeants adverses était aussi importante que les données signalétiques. En outre, il a évoqué des exemples modernes, soulignant comment le renseignement humain a aidé à prévoir et à comprendre des événements complexes, tels que des attaques terroristes ou des mouvements géopolitiques.

L'orateur a conclu cette partie en liant l'importance du renseignement humain aux stratégies de cybersécurité. Il a affirmé que, dans la cybersécurité, comprendre les motivations, les intentions et les comportements humains est aussi vital que de contrer les menaces techniques. C'est le « **perception management** ». Il a souligné que les organisations doivent intégrer une dimension humaine dans leur stratégie de cybersécurité, ce qui implique de prêter attention aux avertissements des sources humaines, de comprendre la psychologie des cyberattaquants et d'anticiper leurs actions.

En conclusion, Bernard Besson a mis en lumière l'importance incontournable du renseignement humain dans la cybersécurité, indiquant que la technologie seule ne peut pas fournir une compréhension complète des menaces. Les organisations doivent donc équilibrer la technologie avec des insights humains pour développer une stratégie de cybersécurité véritablement efficace.

V. La Cybersécurité face aux crises majeures

Dans la cinquième et dernière partie de sa conférence, Bernard Besson a exploré comment les crises majeures, en particulier celles liées à des événements géopolitiques significatifs, influencent la cybersécurité. Il a abordé la manière dont les acteurs de la cybersécurité doivent réagir et s'adapter dans ces situations.

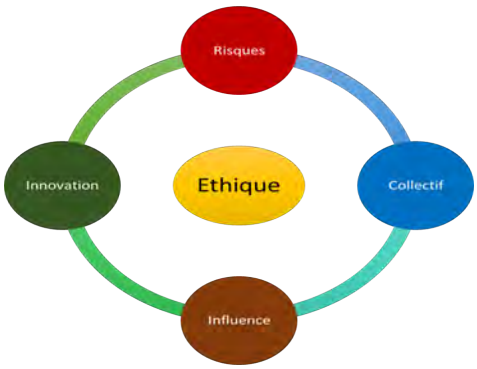
L'intervenant a mis l'accent sur la manière dont des événements tels que les conflits géopolitiques ou les crises majeures transforment le paysage de la cybersécurité. Il a cité des exemples spécifiques, comme le 7 octobre en Israël, pour illustrer comment de telles crises peuvent engendrer des défis uniques pour la sécurité numérique. Il a expliqué que dans de telles situations, les signaux d'alerte peuvent souvent être subtils ou ignorés, conduisant à des réponses inadéquates face aux menaces imminentes.

M. Besson a souligné l'importance d'analyser les signaux faibles dans la prévention des cyberattaques. Il a abordé la nécessité d'une vigilance accrue et d'une analyse minutieuse des informations disponibles pour anticiper et atténuer les effets potentiels des cyberattaques dans un contexte de crise. Il a également mentionné que la compréhension et l'interprétation des signaux faibles sont cruciales pour la préparation et la réponse efficaces aux cybermenaces.

Dans son discours, l'orateur a insisté sur l'importance de l'interprétation des données et de leur présentation aux décideurs politiques. Il a expliqué que les responsables politiques doivent être en mesure de comprendre les implications des menaces de cybersécurité et de prendre des décisions éclairées sur la base de ces informations. Il a abordé le rôle de la cybersécurité et de l'État stratège dans la mise en évidence des menaces et des opportunités cachées, soulignant la nécessité d'une collaboration étroite entre les experts en cybersécurité et les décideurs politiques.

M. Besson a également parlé de la guerre cognitive et de son impact sur la cybersécurité. Il a évoqué comment l'absence d'informations, **le poids du silence et la construction d'influences** jouent un rôle clé dans les stratégies de cybersécurité modernes. Il a souligné que ces aspects souvent négligés sont des terrains inexplorés qui offrent des occasions de collaboration entre la politique et la cybersécurité.

En conclusion de cette partie, Bernard Besson a mis en avant que dans des situations de crise majeure, les défis de la cybersécurité dépassent largement les aspects techniques pour englober des dimensions stratégiques, cognitives et politiques. Il a souligné l'importance d'une approche multidimensionnelle pour anticiper, comprendre et répondre aux menaces dans un monde en constante évolution.



VI. Quelques minutes avec une organisation

Jean-Marc Misert, à la tête du **CLUSIR-GrandEst**, a présenté son organisation lors de la conférence. Le CLUSIR-GrandEst est une association professionnelle dédiée à la cybersécurité et à la diffusion de sa culture. Bien que partageant une partie de son nom avec le CLUSIF national, le CLUSIR-GrandEst fonctionne de manière autonome.

Le CLUSIR-GrandEst compte environ 70 membres, représentant une équivalence en nombre d'entreprises. Cette diversité, allant des petites entreprises aux grandes institutions comme la Banque Postale où travaille M. Misert, offre une richesse d'approches et de perspectives. Leur objectif commun est l'échange de connaissances et d'entraide en cybersécurité.

Les actions menées par le CLUSIR-GrandEst incluent des webinaires thématiques, des réunions en présentiel avec des témoignages de membres ou d'experts extérieurs, et la publication de contenu sur les réseaux sociaux et leur site web. Ces activités sont offertes gratuitement pour maximiser l'accès et la sensibilisation à la cybersécurité.

Le CLUSIR-GrandEst entretient des relations avec d'autres associations, le monde académique, et les sphères étatiques ou territoriales. Ils participent activement dans les réflexions autour de la structuration du futur campus cyber dans le Grand Est, démontrant leur engagement actif dans l'écosystème de la cybersécurité.

M. Misert a exprimé l'ambition de reprendre les colloques annuels, qui étaient des événements de sensibilisation réussis, attirant des centaines de participants. Le but est de toucher à la fois le grand public et les professionnels pour diffuser les meilleures pratiques en matière de sécurité numérique.

Avec une approche inclusive et collaborative, le CLUSIR-GrandEst dirigé par Jean-Marc Misert s'établit comme un acteur clé dans la promotion de la cybersécurité dans la région Grand Est, illustrant l'importance des initiatives régionales dans le renforcement de la sécurité numérique nationale.

VII. Séance de Questions - Réponses

Question 1 :

Intégration de la cyberdéfense et de la guerre électronique face aux menaces numériques hybrides, et intégration de la cybersécurité et de la protection contre les brouillages dans la stratégie de défense actuelle.

Réponse :

Bernard Besson a souligné que les États-Unis sont avancés dans ce domaine, mais la France doit également développer ses capacités. Il a cité l'exemple de l'Ukraine où les Russes utilisent des systèmes de brouillage sophistiqués, démontrant l'importance de ces technologies dans la guerre moderne. Il a insisté sur la nécessité pour les professionnels français de la cybersécurité d'accéder aux connaissances acquises sur le champ de bataille, soulignant l'urgence de cette intégration dans la stratégie de défense française.

Question 2 :

Multiplicité des organismes de cybersécurité en France et leur lien potentiel avec les États-Unis.

Réponse :

L’intervenant a reconnu l'intérêt des États-Unis dans les compétences françaises en cybersécurité. Il a averti que les compétences françaises sont souvent aspirées par les États-Unis, un phénomène qui mérite attention et discussion au sein de la communauté de la

cybersécurité française. Il a suggéré que ces professionnels doivent s'organiser et collaborer avec l'État pour protéger et clarifier leurs intérêts stratégiques.

Question 3 :

La désinformation et la guerre hybride, et la perception erronée des menaces par les politiciens et le public.

Réponse :

Bernard Besson a discuté de la complexité de la situation en Ukraine, expliquant les origines et les développements de la crise. Il a souligné l'importance de comprendre le contexte historique pour mieux appréhender les dynamiques actuelles. Selon lui, la désinformation et le manque de compréhension des enjeux géopolitiques contribuent à une perception déformée des conflits, notamment concernant la Russie.

Question 4 :

La politique industrielle dans le secteur des télécommunications et la cybersécurité, et l'approche entre la concentration industrielle et la concurrence.

Réponse :
L'expert a évoqué la possibilité de revenir à une approche de "planification" inspirée par le modèle du Plan de modernisation et d'équipement d'après-guerre. Il a suggéré que le concept de souveraineté pourrait être un moteur clé pour la cybersécurité, permettant une meilleure coordination entre l'industrie et l'État. Selon lui, les questions de souveraineté et les besoins spécifiques de la France devraient guider les décisions dans le secteur de la cybersécurité.

Conclusion

La conférence de Bernard Besson sur "Etat Stratège et Cybersécurité" a offert une analyse profonde et multidimensionnelle des défis actuels de la cybersécurité dans un contexte mondial complexe. L'expert a mis en lumière la nécessité pour les États de jouer un rôle stratégique actif dans la protection contre les cybermenaces, tout en soulignant l'importance **d'une collaboration étroite entre les secteurs public et privé**.

La conférence a abordé des sujets variés, allant de la gestion des crises majeures et des signaux faibles dans la cybersécurité à l'importance vitale du renseignement humain, en passant par les défis spécifiques posés par les conflits géopolitiques. M. Besson a mis en exergue la complexité des menaces internes et externes et a insisté sur la nécessité de développer une culture de la sécurité robuste et multidimensionnelle, englobant à la fois les aspects technologiques, humains et stratégiques.

En conclusion, la conférence de Bernard Besson a apporté une contribution significative à la compréhension des enjeux contemporains de la cybersécurité. Elle a encouragé **une approche holistique**, impliquant une prise de conscience accrue des implications politiques, stratégiques et humaines de la cybersécurité. L'accent mis sur la formation, la sensibilisation et la

collaboration entre les différentes entités souligne l'importance d'une stratégie globale et intégrée pour contrer efficacement les cybermenaces dans notre monde interconnecté.