CALI-SSI : Challenge Interdisciplinaire en Sécurité des Systèmes d'Information

Romain Xu-Darme

CALI-SSI : CHALLENGE INTERDISCIPLINAIRE EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Romain Xu-Darme
romain.xu(at)univ-grenoble-alpes.fr
Grenoble Alpes Cybersecurity Institute, Univ. Grenoble Alpes

Avec la multiplication des actes de malveillance dans le cyberespace ces vingt dernières années, la cybersécurité a progressivement dépassé le seul domaine technique pour devenir un enjeu politique et économique majeur. Face à ces situations de plus en plus complexes, seule une collaboration entre experts en sécurité informatique, en droit international et en géopolitique peut permettre d'apporter une réponse pertinente dans une approche holistique de la cybersécurité. Dans ce contexte, nous proposons CALI-SSI (prononcer *khaleesi*), un *challenge* de gestion de crise SSI mêlant recueil de preuves numériques et gestion de crise destiné à des équipes mixtes composées d'étudiants en sécurité informatique et en droit international et géopolitique.

***Mots clés*—enseignement, compétition, interdisciplinarité, investigation numérique, gestion de crise.**

I. INTRODUCTION

DEPUIS le début du XXIème siècle et avec la progressive intégration des technologies du numérique au sein de nos sociétés modernes, la cybersécurité est devenue une problématique protéiforme aux enjeux multiples. Enjeux économiques tout d'abord, avec l'apparition d'un marché parallèle de la cyber-criminalité et la création de plateformes d'achat en ligne de vulnérabilités et de données personnelles, mais aussi avec la multiplication d'actes d'espionnage industriel. On assiste également depuis 2019 à une recrudescence de campagnes de rançongiciels ciblant particulièrement les collectivités et leurs infrastructures qui sont bien souvent mal protégées et détentrices de grandes quantités de données personnelles : par exemple Greenville (USA, avril 2019), Baltimore (USA, mai 2019), réseau électrique de Johannesburg (Afrique du Sud, juin 2019), Rennes (France, novembre 2019). Des enjeux idéologiques ensuite avec la multiplication d'actes de cyber-guerre menés par des Etats, que ce soit ouvertement (cyberattaques des USA sur des installations militaires iraniennes) ou bien via l'utilisation d'organisations de cyber-mercenaires très structurées (cyberattaque contre le réseau électrique ukrainien en décembre 2015, cyberattaque lors de la cérémonie d'ouverture des Jeux Olympiques de Séoul par Industroyer en décembre 2016). Ces exemples illustrent un nouveau paradigme de conflit asymétrique où une poignée d'individus peut désormais mettre à mal l'économie d'un pays, voire menacer des vies.

Si des initiatives comme l'*Appel de Paris pour la Confiance et la Sécurité dans le Cyberespace* [1] lancé par le président Emmanuel Macron en novembre 2018 soulignent un début de prise de conscience du monde politique sur les sujets de cybersécurité, une synergie semble nécessaire entre experts techniques, juristes et décideurs politiques au niveau international afin de mettre en place des mesures permettant de garantir la sécurité du bien commun qu'est l'Internet. Ce dialogue n'est pas toujours aisé étant donné la complexité technique du sujet et nécessite la création d'éléments de langage commun entre experts de domaines déconnectés. L'objectif de CALI-SSI est de jeter les bases de cette coopération dès la formation des étudiants à la fois en sécurité informatique et en droit international et géopolitique.

Cette contribution est organisée comme suit : la section II analyse l'existant en matière de compétitions de cybersécurité ; la section III présente le *challenge* CALI-SSI ; enfin, la section IV présente un retour d'expérience sur la première édition du *challenge*.

Ce travail a bénéficié d'une aide de l'Etat gérée par l'Agence Nationale de la Recherche au titre du programme "Investissements d'avenir" portant la référence ANR-15-IDEX-02.

II. UN CLOISONNEMENT DE L'ÉCOSYSTÈME DES COMPÉTITIONS DE CYBERSÉCURITÉ

Avec la nette augmentation du nombre de formations en cybersécurité dans le monde ces dix dernières années, les *challenges* techniques en cybersécurité de type "Capture-the-flag" se sont également multipliés (de 19 en 2011, on en recense 194 en 2019 [2]). Bien qu'une majorité de ces *challenges* soit désormais organisée de manière indépendante en ligne (73 % des *challenges* en 2019), une partie s'effectue néanmoins toujours dans le cadre de conférences en cybersécurité (en France, on peut citer par exemple le Forum International de la Cybersécurité ou encore GreHack), et parfois uniquement pour les étudiants (ex. CSAW ou RESSI). Ces compétitions internationales sont constituées d'un ensemble d'épreuves techniques de cybersécurité mêlant cryptographie, rétro-ingénierie, tests de pénétration, investigation numérique, etc.

Parallèlement, l'Atlantic Council[3] propose quant à lui depuis 2014 le **Cyber 9/12 Strategy Challenge**, orienté sur la prise de décision suite à une cyberattaque. Dans cette compétition, des équipes de quatre étudiants sont confrontées à un scénario fictif de cyber-crise et s'affrontent afin de proposer les meilleures mesures juridiques et politiques à prendre par les autorités pour réagir à la crise. Le scénario évolue au fil de trois actes durant lesquels les étudiants présentent, en anglais et en dix minutes, leurs recommandations devant un jury d'experts en droit international, géopolitique et cyber-stratégie.

Au terme de chaque acte, des équipes sont éliminées jusqu'à la finale où s'affrontent deux ou trois équipes. S'agissant de recommandations de haut niveau en termes de politique de cybersécurité (saisie des instances nationales et internationales compétentes telles que le ComCyber, l'ANSSI, l'ENISA, l'ONU, l'OTAN, etc), ce *challenge* s'adresse essentiellement à des étudiants en droit international et géopolitique, l'aspect technique du scénario étant limité à décrire les effets des actes de cyber-malveillance et non leur mode opératoire (exemple tiré du Challenge du FIC'19 : des pirates informatiques ont réussi à prendre le contrôle des objets connectés du village olympique des JO de Paris 2024 et provoquent des dysfonctionnements à répétition. Les équipes doivent déterminer les mesures juridiques à prendre pour faire cesser l'attaque). A notre connaissance, seul l'Atlantic Council propose un *challenge* de ce type.

Il était frappant de voir au FIC'19 ces deux types de compétitions - *challenge* "Capture-the-flag" destiné aux étudiants des filières techniques d'une part, *Strategy Challenge* destiné aux étudiants des filières juridiques et politiques d'autre part - évoluer physiquement l'une à côté de l'autre dans la zone "Challenge" du bâtiment sans qu'aucune interaction n'ait lieu entre les deux communautés. De ce constat est née l'idée de concevoir un nouveau type de compétition prenant en compte l'aspect interdisciplinaire des crises modernes en cybersécurité et permettant de faire collaborer des étudiants venant de domaines hétérogènes mais aux finalités communes.

III. Construction du *challenge* CALI-SSI

Le *challenge* CALI-SSI est une compétition mêlant intimement recherche de preuves numériques et gestion de crise, où s'affrontent des équipes interdisciplinaires de quatre étudiants (idéalement deux étudiants issus de formations techniques et deux étudiants issus de formation en droit international et/ou en géopolitique [1]), et découpée en deux actes.

Chaque acte est présenté sous forme :

1) d'un scénario fictif décrit au travers de coupures de presse, de mails et d'extraits de réseaux sociaux (page Facebook, fil Twitter, etc) ;
2) d'un ensemble de défis techniques (certains "à tiroir", voir figure 1) dont la résolution permet d'apporter des informations supplémentaires sur la crise (pistes d'attribution de l'attaque, solutions techniques pour résoudre la crise).

A. Acte I - Evaluation de la situation

L'acte I présente les prémices d'une cyber-crise, restreinte dans un premier temps à l'échelle régionale ou nationale, ainsi que des éléments de contexte international, initialement décorrelés de la crise mais qui pourront avoir de l'importance (ou non) lors de l'acte II. L'objectif est d'évaluer la capacité des étudiants à analyser la situation et à en rendre compte à un public non expert.

1. Afin de reproduire des conditions de travail réalistes, la composition de chaque équipe est tirée de manière aléatoire.

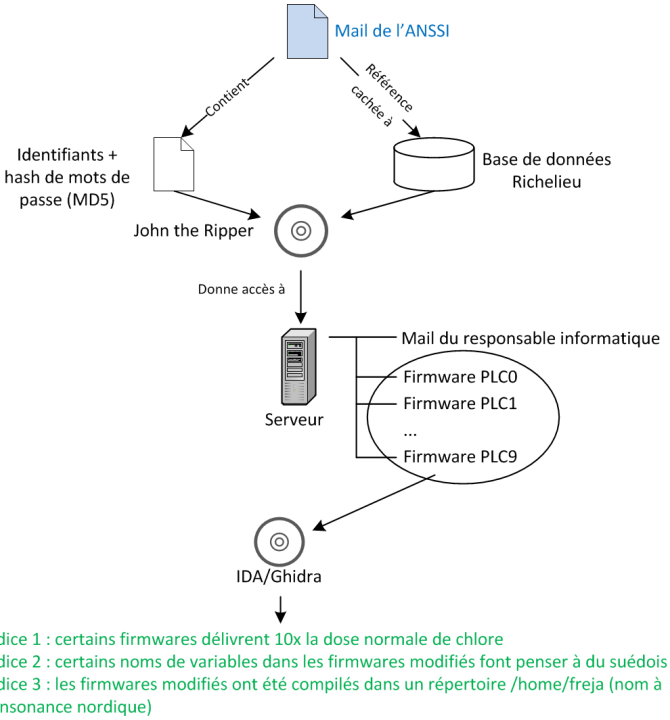

FIGURE 1. Exemple d'extraction d'indices par investigation numérique dans l'acte I : un faux mail de l'ANSSI à destination du SI d'une usine de traitement d'eau - soupçonnée d'être la cible d'une cyberattaque - indique qu'un fichier de mots de passe (sous forme de hashs MD5) a été diffusé sur Reddit. Le mail contient également un lien caché vers la base publique de mots de passe Richelieu qui permet aux étudiants de facilement casser les mots de passe avec JohnTheRipper et d'accéder à un serveur contenant un mail du responsable du SI ainsi que les binaires des automates du système industriel. Une analyse des binaires par Ghidra ou IDA permet de confirmer une cyberattaque et d'extraire des indices sur l'origine de l'attaque.

Rendu attendu Les équipes doivent remettre un rapport écrit de quatre pages maximum à destination du cabinet du premier ministre présentant :

1) Une description globale et synthétique de la situation et de l'étendue de la crise comprenant une évaluation des risques à court, moyen et long termes ;
2) Des pistes d'attribution argumentées sur la base des preuves numériques récoltées avec un niveau de confiance associé ;
3) Des premières suggestions sur les actions à mettre en œuvre à l'échelle nationale et internationale.

Les rapports sont ensuite notés selon la grille présentée dans la table I (même pondération pour tous les thèmes). Selon le nombre d'équipes participant à la compétition, certaines peuvent être éliminées à l'issue de cet acte.

B. Acte II - Réaction

Dans l'acte II, la crise évolue au niveau international et l'objectif pour les étudiants n'est plus de suggérer des mesures préventives mais bien de proposer une ou plusieurs solutions concrètes pour sortir de la crise. Ces solutions peuvent être d'ordre :

TABLE I
GRILLE D'ÉVALUATION

Evaluation des risques	Capacité à déterminer les risques présentés dans le scénario et à évaluer leur gravité et leur probabilité d'occurrence
Investigation numérique	Capacité à résoudre les *challenges* techniques et à associer un niveau de confiance aux preuves numériques récoltées
Originalité des solutions	Capacité à innover dans les suggestions sur les actions à mettre en oeuvre
Qualité de synthèse	Capacité à rendre compte de la situation à un public non expert
Qualité de la présentation	Capacité à convaincre un décideur fictif de mettre en oeuvre les actions proposées (acte II uniquement).

— Technique. ex. Trouver un correctif afin d'endiguer la prolifération d'un malware ;
— Juridique : mise en application de règlements du droit international (ex. transposition du principe de due-diligence dans le cyberespace) ;
— Politique : exercer des pressions diplomatiques ou économiques sur le pays soupçonné d'être à l'origine de la cyberattaque.

Rendu attendu Chaque équipe doit déterminer une ou plusieurs actions concrètes à mettre en oeuvre immédiatement au niveau national et international et les présenter en dix minutes devant un jury d'experts en cybersécurité, géopolitique et droit international. Le jury dispose ensuite de dix minutes pour interroger l'équipe afin d'obtenir des précisions sur les mesures proposées. Les oraux ont idéalement lieu à huis-clos afin d'éviter qu'une équipe ne s'inspire des propositions présentées par les autres. Dans le cas contraire, il est demandé aux équipes de fournir avant le début des oraux un rapport d'une page maximum résumant le contenu de la présentation. Les équipes sont notées selon la grille présentée dans la table I (même pondération pour tous les thèmes) et l'équipe vainqueur est ensuite annoncée.

C. Objectifs pédagogiques

L'objectif de CALI-SSI est de favoriser les interactions entre des étudiants de filières techniques et ceux des filières juridiques ou politiques. Le gain attendu est double : pour les étudiants des filières techniques, le *challenge* permet de remettre la cybersécurité dans un cadre sociétal plus large, donc plus pertinent (qu'a-t-on le droit de faire dans le cyberespace ? l'attribution d'une cyberattaque est-elle une réponse technique ou bien un acte politique ?), mais également de les habituer à communiquer avec un public non expert ; pour les étudiants en droit international et en politique, le *challenge* constitue une initiation aux aspects techniques de la cybersécurité (i.e. la réalité du terrain) afin de mieux appréhender les enjeux de la mise en pratique de certaines régulations du cyberespace.
A plus long terme, l'ambition est de voir apparaître une génération d'ingénieurs et de juristes sensibilisés à des domaines complémentaires à leur formation.

D. Ethique

Problème épineux auquel se heurte la plupart des compétitions techniques de cybersécurité, les considérations éthiques doivent être prise en compte durant la construction du *challenge* et les organisateurs de ce type de compétition font usuellement signer une charte de bonne conduite aux participants. En particulier si l'une des épreuves consiste à analyser un rançongiciel, fournir un code complet et fonctionnel peut mener à une dissémination involontaire [4] et une utilisation à des fins criminelles.
Dans le cas de CALI-SSI, le choix a été fait de fournir uniquement un extrait du logiciel de chiffrement ne contenant :

1) ni le vecteur d'intrusion (clé USB auto-exécutable, PDF) ;
2) ni le code pour l'élévation de privilèges ;
3) ni le code du chiffrement proprement dit (uniquement les appels à une librairie de cryptographie fictive).

Le binaire fourni contenait en revanche des mécanismes issus de véritables rançongiciels tels qu'une coupure d'urgence (découverte par hasard dans Wannacry), une architecture client-serveur pour récupérer la clé de déchiffrement ou encore des bogues volontaires permettant de retrouver la clé de chiffrement en mémoire.

IV. RETOUR D'EXPÉRIENCE SUR LA PREMIÈRE ÉDITION

A. L'Université Grenoble Alpes, un écosystème favorable pour l'expérimentation d'initiatives interdisciplinaires

L'édition pilote de CALI-SSI a été proposée au sein de l'Université Grenoble Alpes, qui propose de nombreuses formations sur des aspects complémentaires de la cybersécurité avec notamment :

— pour la partie technique le Master international CySec (cybersécurité), le Master en alternance CSI (Cybersécurité et Informatique Légale), le Master international MISTRE (sécurité des systèmes embarqués) ;
— pour la partie juridique les Master Sécurité internationale et Défense (SID) et Carrières juridiques internationales (CJI).

Par ailleurs, l'organisation de ce *challenge* a bénéficié de la structuration de la communauté des chercheurs en cybersécurité au sein du Grenoble Alpes Cybersecurity Institute (Cyber@Alps) dont font partie tous les responsables des formations précitées.
Pour des questions d'emploi du temps des formations, le *challenge* a été proposé à la rentrée de septembre 2019 aux étudiants des Masters CSI et SID, sur la base du volontariat.

B. L'édition 2019 en chiffres

TABLE II
CHRONOLOGIE DE LA COMPÉTITION

26 septembre 2019	Date limite des inscriptions / démarrage de l'acte I
13 octobre 2019	Date limite de rendu du rapport de l'Acte I
21 octobre 2019	Démarrage de l'acte II
05 novembre 2019	Oraux de l'acte II et désignation des vainqueurs

13 étudiants (4 étudiants CSI, 9 étudiants SID) ont participé à l'édition 2019 de CALI-SSI. Répartis aléatoirement [2] en

2. Avec la contrainte d'un étudiant CSI par équipe

quatre équipes, tous les étudiants ont participé aux deux actes de la compétition. A l'issue des oraux de l'acte II, 2 équipes ont été sélectionnées pour participer au Strategy Challenge du FIC organisé par l'Atlantic Council fin janvier 2020 à Lille.

C. Premiers retours et pistes d'amélioration

Suite à la compétition, des premiers retours ont été collectés via un questionnaire anonyme remis aux participants. Si ces derniers ont souligné la pertinence du *challenge* par rapport à leur formation (de "Très pertinent" à "Plutôt pertinent"), certains ont déploré un manque de temps de préparation dû à d'autres contraintes de leur emploi du temps. Une intégration de la compétition dans la formation des étudiants [3] permettrait de pouvoir dégager des créneaux dédiés à la préparation des équipes.
Par ailleurs, la récompense du *challenge* - à savoir la participation au Strategy Challenge du FIC'20 - nous a contraints à organiser CALI-SSI très tôt dans l'année scolaire afin de pouvoir sélectionner les vainqueurs avant la fermeture des inscriptions. Sans cette contrainte, il serait pertinent d'organiser ce type de compétition vers janvier, lorsque les étudiants disposent d'un bagage plus avancé dans leur domaine mais avant le départ des élèves ingénieurs en PFE.
Enfin, la gestion de crise ne faisant pas partie des formations CSI ou SID, il serait intéressant d'inclure des étudiants en sciences politiques lors de la prochaine édition.

D. Vers une pérennisation de CALI-SSI

Sur la base de ce retour d'expérience positif, un objectif à court terme est de pérenniser cette compétition au niveau de l'Université Grenoble Alpes en organisant une édition chaque année pour les nouvelles promotions de M2. Un comité d'organisation - composé de chercheurs en droit international, géopolitique et cybersécurité - est actuellement en cours de constitution afin de concevoir un nouveau scénario plus complet pour la prochaine édition.
A plus long terme, le second objectif est d'encourager le développement de ce type d'initiatives dans le monde universitaire à l'échelle nationale. C'est pourquoi l'ensemble du matériel (documents et logiciels) de l'édition pilote est disponible sur demande par mail à l'auteur.

CONCLUSION

Nous avons présenté CALI-SSI, un *challenge* qui, à notre connaissance, n'a pas d'équivalent aujourd'hui dans l'écosystème des compétitions en cybersécurité et qui mêle des aspects techniques, juridiques et géopolitiques dans un scénario de crise réaliste. Le but de cette compétition est de favoriser l'interdisciplinarité et de bâtir des ponts entre étudiants de domaines connexes pour une approche holistique de la cybersécurité.

3. L'édition pilote était basée sur le volontariat

REMERCIEMENTS

L'auteur voudrait remercier Cyril Bras (RSSI de la Grenoble Alpes Métropole), Pascal Lafourcade (Université de Clermont-Auvergne), Jérôme Mercier et Florent Autréau (Université Grenoble Alpes) pour leur aide dans la création du scénario et des épreuves techniques, ainsi que Philippe Elbaz-Vincent et Karine Bannelier-Christakis (Université Grenoble Alpes) pour avoir permis aux étudiants de CSI et de SID de participer à ce *challenge*.

RÉFÉRENCES

[1] "Appel de Paris pour la confiance et la sécurité dans le cyberespace." [Online]. Available : https ://pariscall.international/fr/

[2] CTF Time, "CTF events." [Online]. Available : https ://ctftime.org/event/list/past

[3] Atlantic Council, "Cyber 9/12 Strategy Challenge." [Online]. Available : https ://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/

[4] J. Snow, K. Kochetkova, A. Stern, and M. Sobolevskaya, "Comment un projet éducatif open-source s'est converti en un ransomware dangereux appelé Ded Cryptor." [Online]. Available : https ://www.kaspersky.fr/blog/ded-cryptor-ransomware/5797/