La conflictualité cyber
Nouveaux conflits dans d'autres théâtres, ou nouveaux théâtres des mêmes conflits ?

Présentation du séminaire

Les deux premières décennies du 21e siècle, marquées par la numérisation croissante des sociétés et des économies, ont vu le cyberespace s'affirmer comme un nouveau champ de confrontation stratégique, où se traduit le regain de la compétition géopolitique entre Etats. En multipliant les « zones grises » qui brouillent le champ et la définition de la guerre, le cyberespace devient ainsi le théâtre d'une nouvelle forme de conflictualité soulevant des défis spécifiques : quelle réponse apporter à des incidents se situant souvent sous le seuil du recours à la force armée ? Comment prévenir les risques d'escalades et de conflits armés pouvant naître d'un incident cyber ? Comment élaborer des normes permettant de régir la conduite des Etats dans le cyberespace ? Comment lutter efficacement comme la prolifération des armes cybernétiques ?

Ce séminaire sera animé par Yves Verhoeven, Sous-Directeur Stratégie de l'ANSSI et Hugo Zylberberg, Chef du Pôle Analyses Stratégiques à la Sous-Direction Stratégie. Il permettra aux étudiants de découvrir ou d'approfondir leur compréhension du domaine cyber, tout en explorant les dynamiques, nouvelles et persistantes, de la conflictualité cyber et en abordant les efforts mis en œuvre au niveau international pour réguler cette conflictualité. A l'issue du semestre, les étudiants seront capables de comprendre les dynamiques géopolitiques du champ cyber, d'analyser les évolutions de la conflictualité cyber et des mécanismes de régulation internationale à l'œuvre.

Fonctionnement du séminaire

Chaque cours commencera par des résumés rapides des lectures obligatoires et des lectures « distribuées » à l'un des étudiants. La littérature sur laquelle s'appuie le cours est très largement rédigées en anglais, et les intervenants seront francophones et anglophones.

La note finale du séminaire prendra en compte la participation orale aux synthèses des lectures ainsi que l'essai final demandé.

Dates des séances du séminaire

- 26 janvier, 18-20h
- 9 février, 18-20h
- 9 mars, 18-20h
- 23 mars, 18-20h
- 6 avril, 18-20h
- 20 avril, 18-20h

Essai final

Les étudiants s'appuieront sur le séminaire pour rédiger un essai de 3000 mots sur l'un des trois sujets suivants :

- ➔ 1er sujet : En vous appuyant sur des exemples de votre choix, quelles sont les caractéristiques fondamentalement nouvelles de la conflictualité cyber qui vous semblent mériter de nouvelles approches conceptuelles ?

- ➔ 2e sujet : En vous appuyant sur des exemples de votre choix, quelles sont les caractéristiques de la notion de territoire qui vous semblent les plus pertinentes pour analyser la conflictualité cyber ?

- ➔ 3e sujet : En vous appuyant sur des exemples de votre choix, comment les Etats devraient-ils adapter leur façon de gérer la sécurité et la stabilité internationale pour mieux prendre en compte le fait cyber ?

Premier cycle : De la guerre au conflit, une évolution conceptuelle

Séance N°1 (26 janvier) : Introduction – définition et caractéristiques du cyberespace

Lors de ce premier cours, nous définirons le cyberespace et présenterons les caractéristiques principales de cet espace stratégique contesté qui devient le lieu d'affirmation des puissances à travers une présentation d'incidents majeurs. Nous discuterons ensuite de la façon dont des concepts fondamentaux tels que la prolifération, la dissuasion et la puissance des Etats se traduisent dans le cyberespace.

- *Intervenant : [A définir]*

Lectures obligatoires (79 pages) :
- (13 pages) Julien Nocetti, « Géopolitique de la cyber conflictualité. » *Politique Etrangère*, 2 :2018.
  - Disponible en ligne : https://www.ifri.org/sites/default/files/atoms/files/geopolitique_de_la_cyber-conflictualite.pdf
- (19 pages) Joseph Nye, "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly 5:4*, Hiver 2011 (pp. 20-38).
  - Disponible en ligne : https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-4/Winter11.pdf
- (19 pages) Joseph Nye, « Cyber Power.» *Belfer Center*, 2016.
  - Disponible en ligne : https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf
- (28 pages) Joseph Nye, "Deterrence and Dissuasion in Cyberspace." *International Security 41:3*, 2016.
  - Disponible en ligne : https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf

Lectures distribuées :
- (6 pages) John Arquilla. "Cyberwar Is Already Upon Us." *Foreign Policy*, March/April, 2012.
  - Disponible en ligne : http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us
- Rapports d'analyse de la menace
  - (7 pages) Nicolas Falliere, Liam O Murchu, and Eric Chien. *W32.Stuxnet Dossier*, Version 1.4, février 2011 (pp. 1-7).
    - Disponible en ligne : https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
  - (7 pages) Kaspersky, "Equation Group: Questions And Answers." Février 2015 (pp. 3-4, 15-18, 31).
    - Disponible en ligne : https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
  - (27 pages) Mandiant, « APT1 : Exposing One of China's Cyber Espionage Units. » Février 2013 (pp. 1-27).
    - Disponible en ligne : https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
  - (17 pages) F-Secure Labs Threat Intelligence, « The Dukes, 7 years of Russian cyberespionage. » Septembre 2015 (pp. 1-15, 26-27).
    - Disponible en ligne: https://labs.f-secure.com/assets/BlogFiles/dukes-whitepaper.pdf

Séance N°2 (9 février) : Le domaine cyber est le théâtre d'une nouvelle forme de conflictualité entre Etats

Nous aborderons dans cette séance les dynamiques nouvelles du conflit cyber et les principaux incidents de cybersécurité historiques sous des angles opérationnels, tactiques et stratégiques. A travers une série d'attaques historiques (Vault7, Mirai, OPM, DDoS Dyn, DNC hack, SolarWinds / Kaseya, APT31 – Exchange), nous expliquerons l'accumulation des surprises stratégiques dans ce nouveau domaine de conflictualité. Nous remarquerons que ces incidents interviennent sous le seuil de la force, et nous analyserons de quelle façon ces incidents remettent en question certains des dogmes initiaux concernant le domaine cyber ("Digital Pearl Harbor" → Colonial Pipeline, « Cyberattacks are becoming easier" → NotPetya, « Massive Collateral Damage » → WannaCry, « Offense Dominates Defense » → Rançongiciels, « Cyberarms Control Agreement » → Pegasus) et exigent d'inventer des concepts nouveaux pour appréhender ces nouvelles dynamiques.

- *Intervenant : [A définir]*

Lectures obligatoires (66 pages) :

- (12 pages) Matthias Schulze, Josephine Kerscher, Paul Bochtler. "Cyber Escalation – The conflict dyad USA / Iran as a test case." *SWP Working Paper*, Décembre 2020.
    - Disponible en ligne : https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Schulze_December20_Cyber_Escalation_Research_01.pdf
- (24 pages) Thomas Rid. "Think Again: Cyberwar." *Foreign Policy*, March/April, 2012.
    - Disponible en ligne : http://www.foreignpolicy.com/articles/2012/02/27/cyberwar
- (22 pages) Max Smeets (2018) "A matter of time: On the transitory nature of cyberweapons," *Journal of Strategic Studies, 41:1-2, 6-32*.
    - Disponible en ligne : https://doi.org/10.1080/01402390.2017.1288107
- (8 pages) Matthias Schulze. « Cyber Deterrence is Overrated. » *SWP Comment,* N°34, Août 2019.
    - Disponible en ligne : https://www.swp-berlin.org/publications/products/comments/2019C34_she.pdf

Lectures distribuées :

- (12 pages) Michael P. Fischerkeller, Richard J.Harknett, "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis 61:3*, 2017.
    - Disponible en ligne : https://doi.org/10.1016/j.orbis.2017.05.003
- (15 pages) Lessig, "The Laws of Cyberspace." 1998.
    - Disponible en ligne : https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf
- (12 pages) Douzet Frédérick, Géry Aude, « Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace », *Hérodote, 2020:2-3, 329-350*.
    - Disponible en ligne : https://www.cairn.info/revue-herodote-2020-2.htm

Deuxième cycle : la souveraineté dans le cyberespace - un Internet mondialisé ou des Internets territorialisés ?

Séance N°3 (9 mars) : Souveraineté dans le cyberespace et gouvernance de l'Internet

Le cyberespace, par nature virtuel et déterritorialisé, remet en cause les conceptions traditionnelles de la souveraineté de l'Etat. Au cœur de la notion de souveraineté, l'avènement d'Internet, avec l'utopie d'un espace universel unique et complètement déterritorialisé, met au défi les Etats qui cherchent, soit à en reprendre le contrôle pour mettre en œuvre leurs objectifs stratégiques, soit à en protéger le cœur public (*public core of the Internet*). Ces tensions s'illustrent à travers de nombreuses problématiques actuelles : comment coopérer avec les acteurs d'Internet et avec les acteurs privés, comment l'Etat peut-il protéger ses citoyens face aux menaces en ligne (régulation des contenus, accès aux données de chiffrement, criminalité organisée) ? Nous tenterons également de percevoir quelles stratégies les Etats mettent en place pour le contrôle des infrastructures physiques du numérique. Dans quelle mesure la fracturation du numérique est-elle une réalité et quelles en seraient les conséquences géopolitiques ?

- *Intervention : Henri Verdier*

Lectures obligatoires (58 pages) :

- Yahoo !
    - (9 pages) Jack Goldsmith, Tim Wu, "Who Controls The Internet: Illusions of a Borderless World." Oxford University Press, 2006, pp. 1-10.
        - Disponible en ligne : https://books.google.fr/books?id=zkT9CQAAQBAJ&printsec=frontcover&hl=fr#v=onepage&q&f=false
- IANA Transition
    - (7 pages) L. Gordon Crovitz, « America's Internet Surrender ». *Wall Street Journal*, Mars 2014.
        - Disponible en ligne : https://www.wsj.com/articles/SB10001424052702303563304579447362610955656
    - (9 pages) Jonathan Zittrain, « No, Barack Obama Isn't Handing Control of the Internet Over to China ». *The New Republic*, Mars 2014.
        - Disponible en ligne : https://newrepublic.com/article/117093/us-withdraws-icann-why-its-no-big-deal
- Coeur public de l'internet
    - (33 pages) Dennis Broeders, "The public core of the Internet – An International Agenda for Internet Governance." WRR Report, 2015, pp. 31-64,

- Disponible en ligne : https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

Lectures distribuées :

- (4 pages) John Perry Barlow, A Declaration of the Independence of Cyberspace. 1996.
  - Disponible en ligne : https://www.eff.org/fr/cyberspace-independence

Séance N°4 (23 mars) : Les champs de fracturation du cyberespace, une cyber guerre froide ? Etudes de cas

A travers une série d'étude de cas à différents niveaux de l'architecture d'Internet, nous tenterons de percevoir quelles stratégies les Etats mettent en place afin d'imposer la notion de frontière dans le cyberespace et de préserver leur pouvoir.

Etudes de cas :

- Infrastructures territorialisées : Câbles sous-marins
- Frontières logiques : BGP
- Barrières politiques : enjeux de souveraineté liés à l'informatique nuagique
- Régionalisation sociale : fragmentation en blocs régionaux (ex : Ru.net)

- *Interventions : Deux jeunes chercheurs viendront présenter leurs études de cas*

Lectures distribuées :

- Frontières physiques :
  - (16 pages) Charles Perragin & Guillaume Renouard, « Les câbles sous-marins, une affaire d'États - Quand l'infrastructure des réseaux redevient géopolitique. » *Le Monde diplomatique*, Juillet 2021.
    - Disponible en ligne : https://www.monde-diplomatique.fr/2021/07/PERRAGIN/63256
  - (8 pages) Emily Clark, "Undersea cables bring Pacific nations online, but there are concerns China is trying to tap in." *ABC News*. Juillet 2021.
    - Disponible en ligne : https://www.abc.net.au/news/2021-07-24/china-huawei-build-png-cable-that-connects-to-sydney/100249922
  - (20 pages) Félix Blanc, « Géopolitique des câbles : une vision sous-marine d'internet. » *CAPS*, 2018.
    - Disponible en ligne : https://www.diplomatie.gouv.fr/IMG/pdf/6_carnets_26_dossier_geopolitique_cables__cle43116d.pdf
- Frontières logiques :
  - Limonier, K., Douzet, F., Pétiniaud, L., Salamatian, L., & Salamatian, K. "Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine." *First Monday 26:5*, 2021.
    - Disponible ici : https://journals.uic.edu/ojs/index.php/fm/article/view/11700/10128
- Cloud :
  - (15 pages) Bômont Clotilde, Cattaruzza Amaël, « Le cloud computing : de l'objet technique à l'enjeu géopolitique. Le cas de la France », *Hérodote, 2020:2-3, 149-163*.
    - Disponible en ligne : https://www.cairn.info/revue-herodote-2020-2.htm
- Fragmentation :
  - (16 pages) Kevin Limonier, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », *EchoGéo*, 25 juin 2021.
    - Disponible en ligne : http://journals.openedition.org/echogeo/21804

Troisième cycle : assurer la sécurité et la stabilité internationale malgré la conflictualité cyber

Séance N°5 (6 avril) : L'évolution des stratégies de puissance des grands Etats

Lors cette séance, nous ferons un panorama des stratégies de puissance des Etats dans le cyberespace, avec un focus particulier sur le modèle français de cyberdéfense. Après avoir comparé ces stratégies de puissance, nous analyserons enfin un nouvel élément stratégique susceptible de façonner l'évolution de la conflictualité dans les prochaines années : l'émergence de la grande criminalité cyber (rançongiciels) et les manipulations de l'information (Russie et Chine).

- *Intervention : Anne Tricaud*

Lectures distribuées :

France (20 pages)

- (14 pages) Revue stratégique de cyberdéfense, Mars 2018, pp. 38-42, 43-51.
    - Disponible en ligne : http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
- (6 pages) François Delerue, Aude Géry, « Le droit international dans la *Stratégie Nationale de la Cyberdéfense*. » *IRSEM*, Note de recherche n°58, 11 juillet 2018.
    - Disponible en ligne : https://www.irsem.fr/data/files/irsem/documents/document/file/2429/NR%20IRSEM%2058%20-%20Delerue%20-%20Droit%20international.pdf

Etats-Unis (43 pages)

- (9 pages) **US** "Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command"
    - Disponible en ligne : https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010
- (10 pages) Richard J. Harknett, "United States Cyber Command's New Vision: What It Entails and Why It Matters." *Lawfare*, Mars 2018.
    - Disponible en ligne https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters
- (8 pages) Herb Lin, Max Smeets, " What Is Absent From the U.S. Cyber Command 'Vision'". *Lawfare*, Mai 2018.
    - Disponible en ligne : https://www.lawfareblog.com/what-absent-us-cyber-command-vision
- (16 pages) Taillat Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », *Hérodote, 2020:2-3, 313-328*.
    - Disponible en ligne : https://www.cairn.info/revue-herodote-2020-2.htm

Union Européenne (25 pages)

- The EU's Cybersecurity Strategy for the Digital Decade, Décembre 2020.
    - Disponible en ligne : https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

Royaume-Uni (20 pages)

- National Cyber Security Strategy 2016-2021. 2016, pp8-11, 12-15, 24-31, 62-65.
    - Disponible en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Russie (41 pages)

- (11 pages) Doctrine of Information Security of the Russian Federation, Décembre 2016.
    - Disponible en ligne : https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163
- (30 pages) J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, « Les Manipulations de l'information : un défi pour nos démocraties. » *Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées,* Août 2018, pp. 43-63
    - Disponible en ligne : https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf

Chine (36 pages)

- (10 pages) International Strategy of Cooperation on Cyberspace, Décembre 2016.
    - Disponible en ligne : https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml
- (12 pages) National Cyberspace Security Strategy (traduction non-officielle). Décembre 2016.
    - Disponible en ligne : https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/
- (14 pages) Dennis Broeders, Liisi Adamson and Rogier Creemers, "A coalition of the unwilling? Chinese and Russian perspectives on cyberspace", November 2019.
    - Disponible en ligne : https://www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace

Séance N°6 (20 avril) : La réponse multilatérale au fait cyber

Cette dernière séance aura pour objet de présenter les principales négociations multilatérales menées, notamment dans le cadre des Nations unies, pour renforcer la sécurité et la stabilité internationales dans le cyberespace ; d'analyser les principaux enjeux et difficultés des discussions dans ces enceintes (applicabilité du droit international au cyberespace, débats concernant l'attribution des cyberattaques, rôle des acteurs privés, etc.) ainsi que les perspectives pour la régulation internationale de la conflictualité cyber.

- La gouvernance du cyberespace dans les instances internationales
- Les instances de normalisation / standardisation
- L'Union européenne
- Autres mécanismes internationaux pertinents

- *Intervention : Paul Zajac*

Lectures obligatoires (37 pages) :
- (15 pages) Joseph Nye, "The Regime Complex for Managing Global Cyber Activities," *Belfer Center*, Novembre 2014.
    - Disponible en ligne https://www.belfercenter.org/sites/default/files/files/publication/global-cyber-final-web.pdf
- (8 pages) Patryk Pawlak, Eneken Tikk, Mika Kerttunen, « The EU and conflict prevention in cyberspace." *EUISS Conflict Series*, Brief 7, Avril 2020.
    - Disponible en ligne : https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%207_Cyber.pdf
- (11 pages) Patryk Pawkal, « Protecting and defending Europe's cyberspace. » *EUISS Chaillot Papers*, Chapitre 10, Octobre 2018.
    - Disponible en ligne : https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf
- Communiqués relatifs aux activités d'APT 31 / APT 40
    - (1 page) Antony J. Blinken, Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace. 19 juillet 2021.
        - Disponible en ligne : https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/
    - (1 page) Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise. 19 juillet 2021.
        - Disponible en ligne : https://www.nato.int/cps/en/natohq/news_185863.htm
    - (1 page) China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory. 19 juillet 2021.
        - Disponible en ligne : https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/pdf

Lectures distribuées :
- (7 pages) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2010 Report (A/65/201).
    - Disponible en ligne : https://undocs.org/A/65/201
- (10 pages) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 Report (A/68/98).
    - Disponible en ligne : https://undocs.org/A/68/98
- (4 pages) 2015 SCO International Code of Conduct for State Behaviour in information security.
    - Disponible en ligne : https://undocs.org/A/69/723
- (13 pages) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 Report (A/70/174).
    - Disponible en ligne : https://undocs.org/A/70/174
- (17 pages) Advance copy of the 2021 GGE report.
    - Disponible en ligne : https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf
- (11 pages) Conference Room Paper of the OEWG 2021.
    - Disponible en ligne : https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf