

2025.04.16 - Bloc 3 - Cours Les impacts informatiques lors de conflit géopolitique ou guerre

**



Yohan Ranson

Espionnage numériques américain envers l'Europe (Affaire Snowden)

Introduction

En 2013, Edward Snowden, ancien employé de l'Agence de Sécurité Nationale américaine (NSA), révèle au monde entier un programme massif d'espionnage numérique organisé par les États-Unis. Ces révélations ont mis en lumière des pratiques intrusives visant non seulement les ennemis potentiels des États-Unis, mais aussi leurs alliés européens, générant un véritable scandale international.

(Source : Le Monde)

Chronologie des événements

- Juin 2013 : Edward Snowden transmet des documents confidentiels à des journalistes, révélant l'existence du programme PRISM permettant à la NSA d'accéder directement aux données des géants technologiques américains.
- Octobre 2013 : Il est découvert que le téléphone personnel d'Angela Merkel, chancelière allemande, était surveillé par les États-Unis depuis au moins 2002.
- Réaction immédiate : Cette révélation provoque une crise diplomatique majeure entre les États-Unis et plusieurs pays européens, affectant profondément la confiance mutuelle et les relations diplomatiques.

(Source : France24)

Techniques utilisées par la NSA

- Interception massive des communications : La NSA intercepte systématiquement les appels téléphoniques, les SMS, les courriels ainsi que d'autres communications électroniques, analysant à grande échelle des données personnelles.
- Programme PRISM : Grâce à PRISM, la NSA avait un accès direct et privilégié aux données stockées par les plus grandes entreprises technologiques américaines, telles que Google, Apple, Microsoft et Facebook, permettant une surveillance globale des individus ciblés.

(Source : France Info)

Conséquences géopolitiques

- Perte de confiance entre alliés : Ces révélations ont profondément ébranlé les relations diplomatiques entre les États-Unis et leurs alliés européens, semant le doute sur la fiabilité des États-Unis comme partenaire.
- Réaction européenne immédiate : Pour protéger leurs citoyens et leurs institutions, les pays européens ont accéléré la mise en place du Règlement Général sur la Protection des Données (RGPD), lancé des projets pour développer un « cloud souverain européen », et renforcé considérablement leurs politiques nationales en matière de cybersécurité.

(Sources : Le Monde, France24)

Perspectives futures

- Renforcement de la souveraineté numérique européenne : Les pays européens investissent davantage dans des infrastructures numériques sécurisées pour protéger leur souveraineté numérique face aux risques d'espionnage international.

- Persistance des tensions diplomatiques : La méfiance continue de subsister sur la question de la surveillance numérique, affectant durablement les relations entre alliés occidentaux.
- Vigilance accrue envers les technologies étrangères : L'Europe adopte désormais une approche plus prudente et restrictive envers les technologies étrangères potentiellement compromises, telles que la 5G, l'intelligence artificielle et les solutions de Cloud.

(Sources : analyses personnelles inspirées des conséquences rapportées par France Info et Le Monde)



**