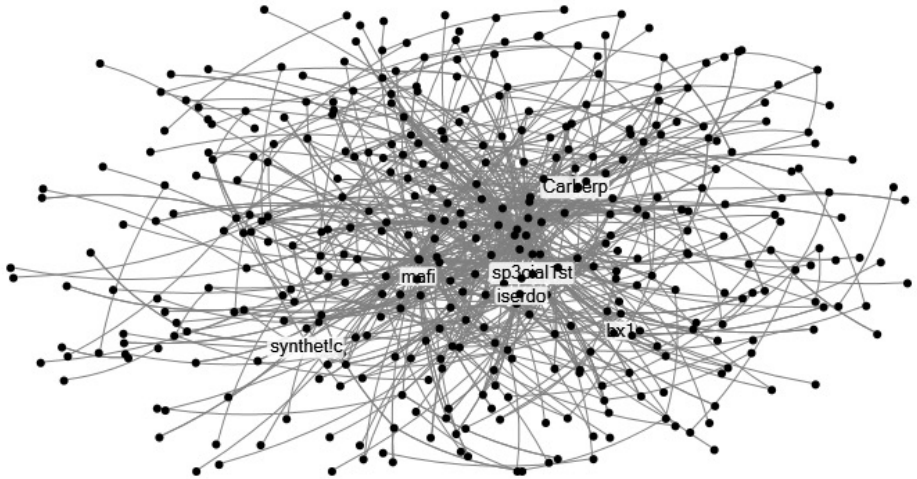
La coévolution : dynamiques de l'innovation dans l'écosystème du cybercrime

Benoît Dupont

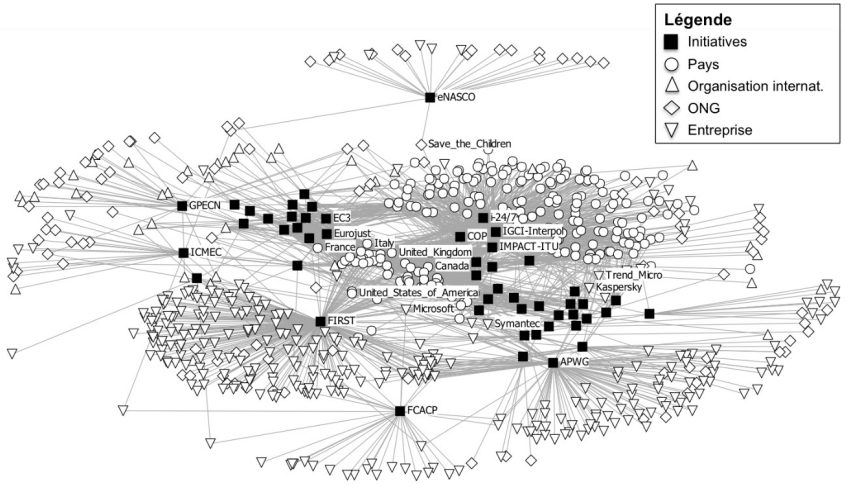
Université de Montréal

Un monde de réseaux

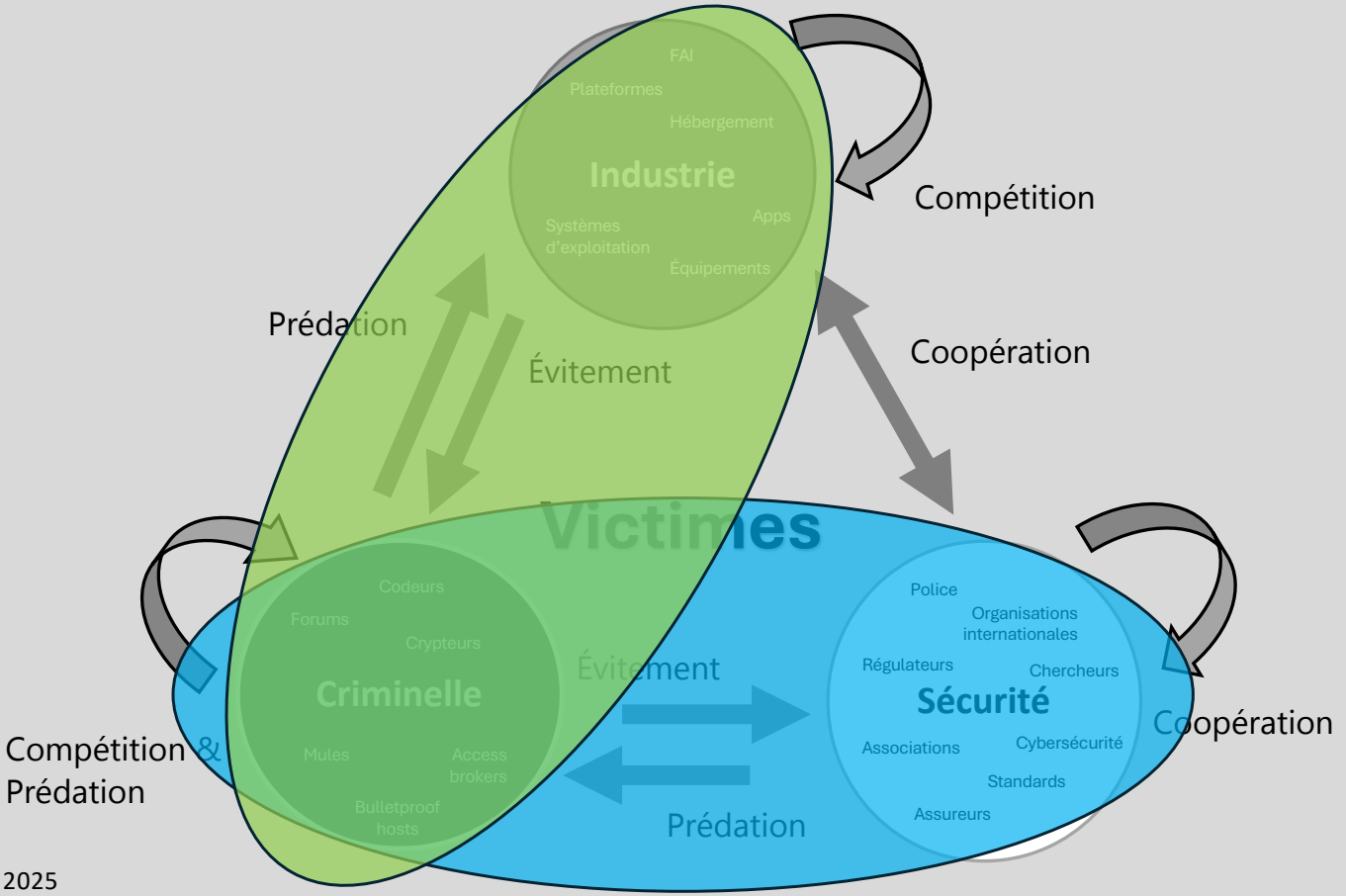
Dark0de



Coopération policière



Un écosystème d'interactions

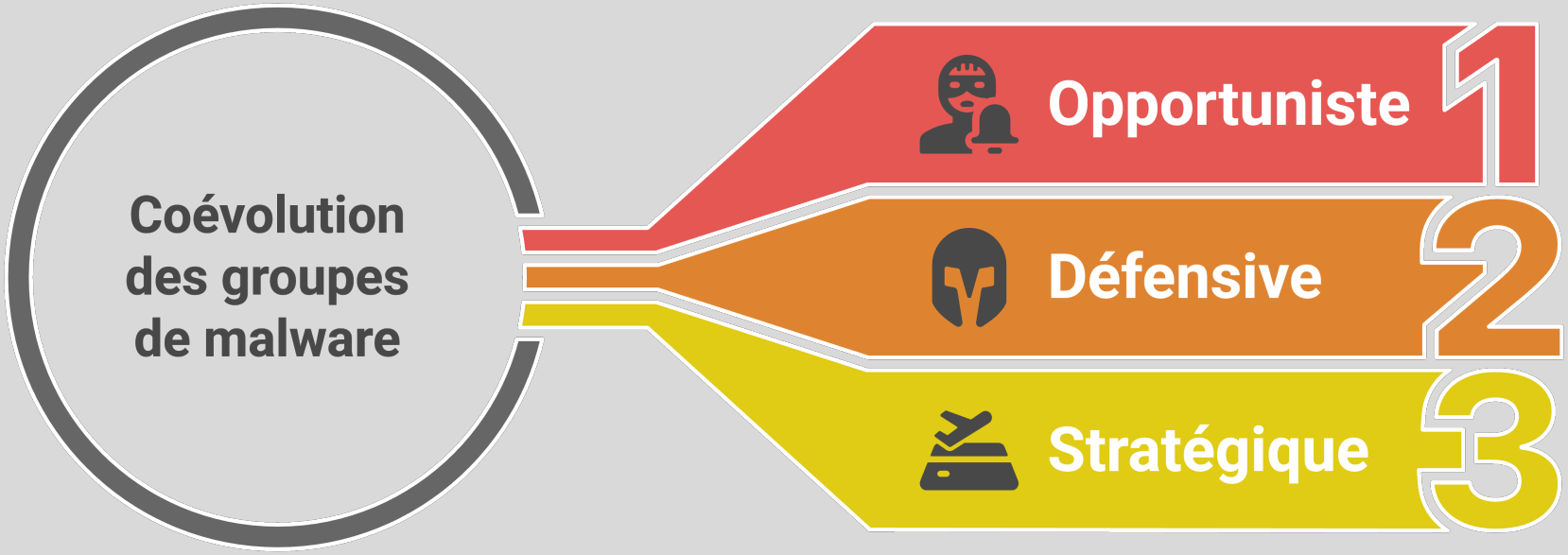


Coévolution crime-sécurité

L'adaptation réciproque de groupes mutuellement interdépendants qui résulte de leurs interactions soutenues

La coévolution des groupes sociaux ou organisationnels est un processus beaucoup plus rapide que dans le monde biologique, où les espèces évoluent très lentement : innovation humaine

3 configurations coévolutives du cybercrime



La coévolution opportuniste

La confusion du possible et du probable

Subject: Custom Benefits Insurance Group Open Benefits Enrollment for [redacted]. Please complete attached per Custom Benefits Insurance Group instructions before close date July 5, 2023
From: Custom Benefits Insurance Group <alerts@pssalerts.info>
To: [redacted]
Reply-to: m[redacted]@gmail.com <m[redacted]@gmail.com>
Date: July 4, 2023, 7:30am ET

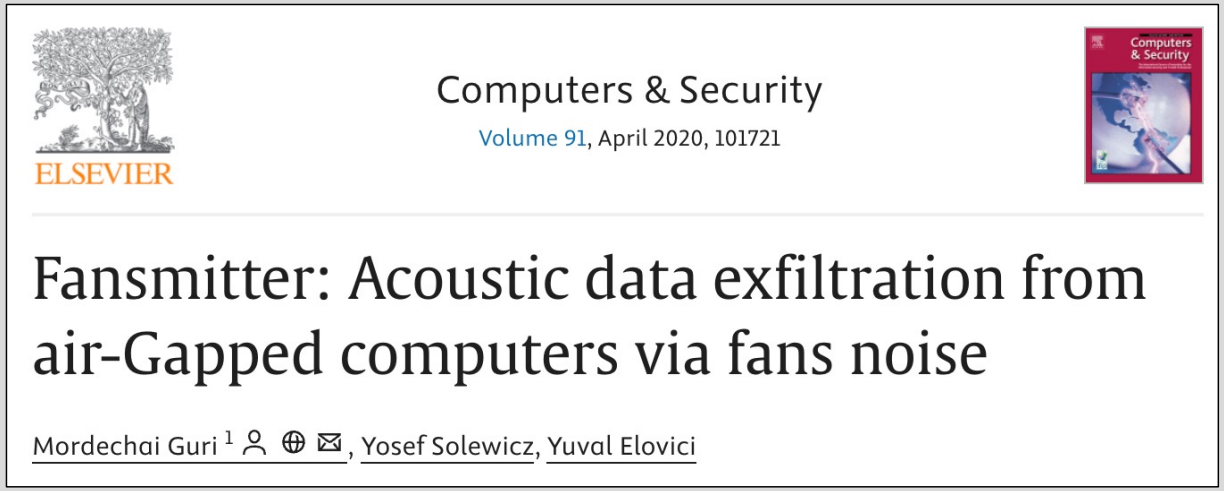
Hi [redacted],

Attached to this letter, you will find the Custom Benefits Insurance Group Benefits Enrollment Form. This document outlines the various Custom Benefits Insurance Group benefits options available to you, including health insurance, retirement plans, flexible spending accounts, and other valuable benefits. Please take the time to carefully review the provided information and consider your individual needs and circumstances.
When completing the Benefits Enrollement Form, please ensure that all required fields are filler out accurately and completely. Any missing or incomplete information may result in a delay in processing your enrollement or could potentially impact your benefits coverage.
Should you have any further questions or need additional information, please feel free to reach out. We are here to assist you.
Best regards,

Custom Benefits Insurance Group

La coévolution opportuniste

Recherche de l'efficience (loi du moindre effort), par contraste avec l'innovation permanente attribuée aux cybercriminels



ELSEVIER

Computers & Security

Volume 91, April 2020, 101721

Fansmitter: Acoustic data exfiltration from air-Gapped computers via fans noise

Mordechai Guri [1], Yosef Solewicz, Yuval Elovici

Exploitation parasitaire de la communauté de la sécurité

Hacking Team >> Angler [Lurk]

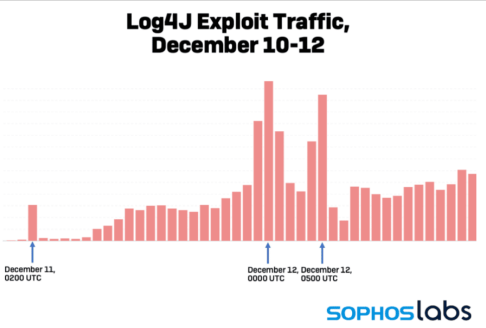
Angler EK Exploits

In 2015, Angler EK began focusing on exploits targeting three applications: Flash player, Internet Explorer, and Silverlight. Angler is often one of the first EKs to use new exploits targeting these applications.

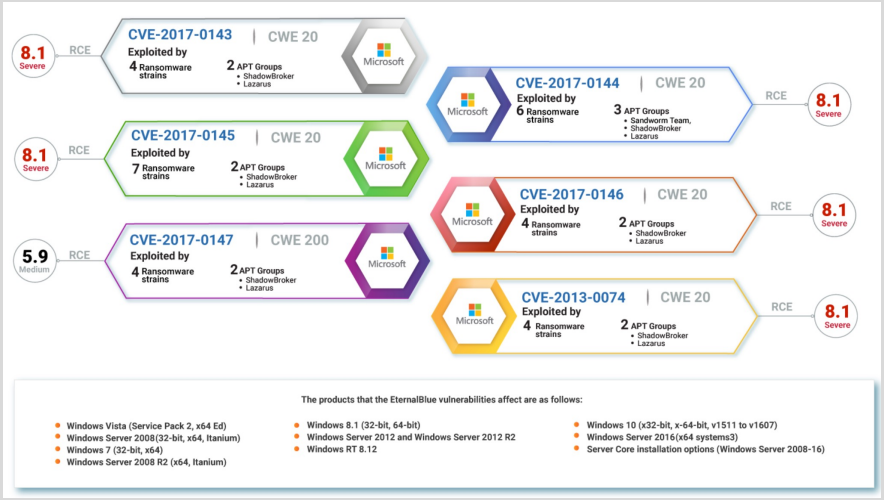
For example, in June 2015 a previously unknown Flash vulnerability (later identified as CVE-2015-5119) was part of some 400 gigabytes of data dumped on the Internet as **part of the infamous Hacking Team breach**. A Flash exploit based on CVE-2015-5119 was integrated into Angler EK **hours after the data dump was publicly available**. It was a zero-day exploit at least 24 hours in the wild before Adobe issued a patch for it.

By August 2015, Angler EK **implemented an exploit for Internet Explorer (IE) vulnerability CVE-2015-2419** that Microsoft had patched the previous month.

In February 2016, **exploits for Silverlight based on CVE-2016-0034** found their way into Angler EK a little more than a month after Microsoft issued a patch for the vulnerability.



L'héritage EternalBlue [NSA]



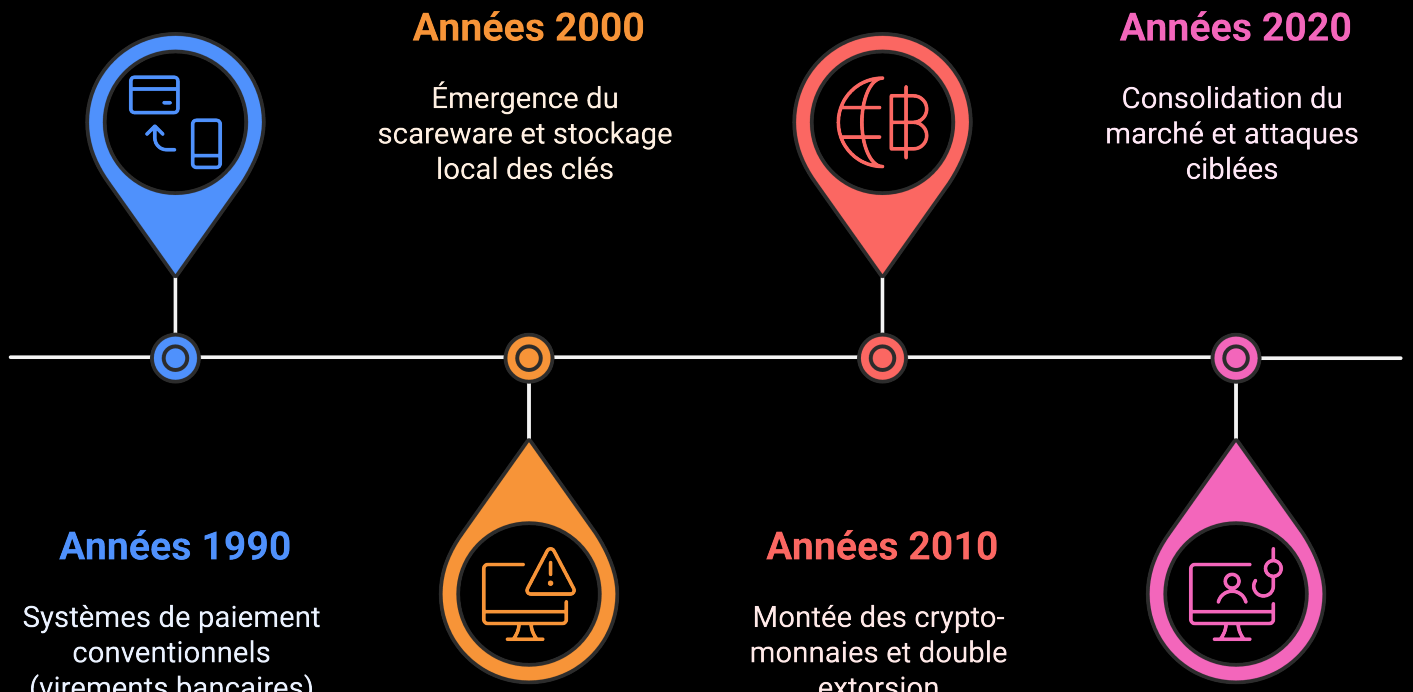
Log4Shell [botnets, cryptomining, exfiltration de données]

La coévolution défensive

Survie

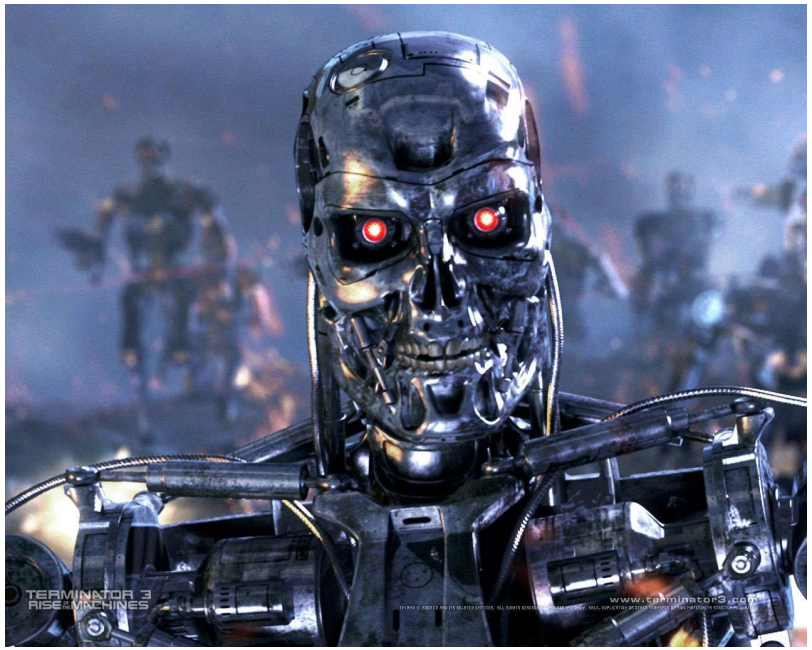
Mimétisme: essayer de paraître légitime (cloud)
Modification: adaptation aux conclusions et rapports de cybersécurité
Contre-détection: surveillance des environnements numériques
Évitement: éviter de révéler des activités lors de l'interaction avec des machines suspectes
Mouvement: Changement d'adresses IP et de techniques de cryptage à intervalles réguliers
Perturbation: introduction de bruit dans les données
Fragmentation: segmentation des infrastructures techniques

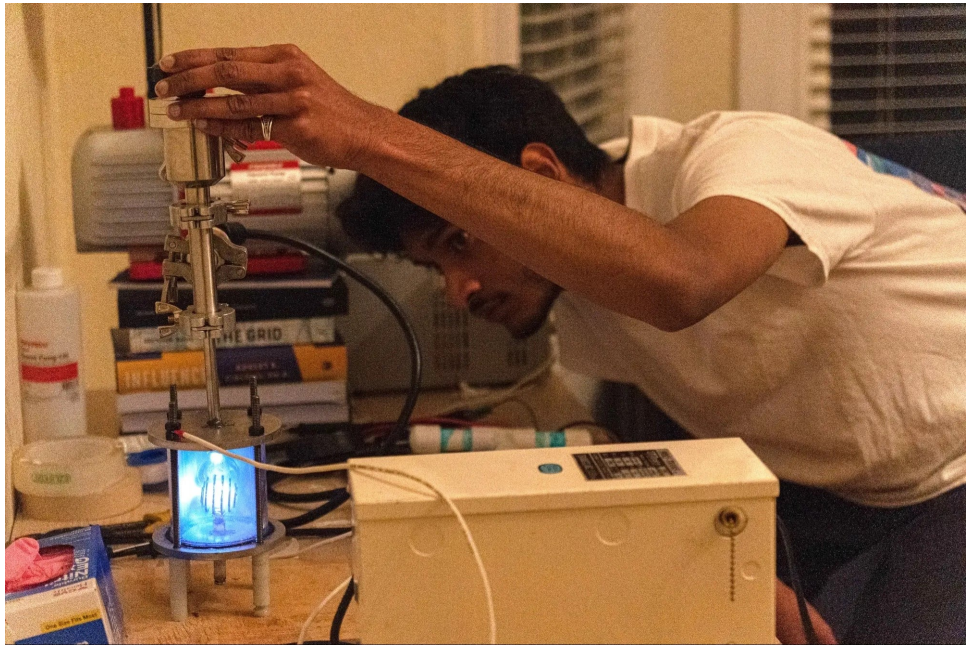
La coévolution stratégique (efficacité)



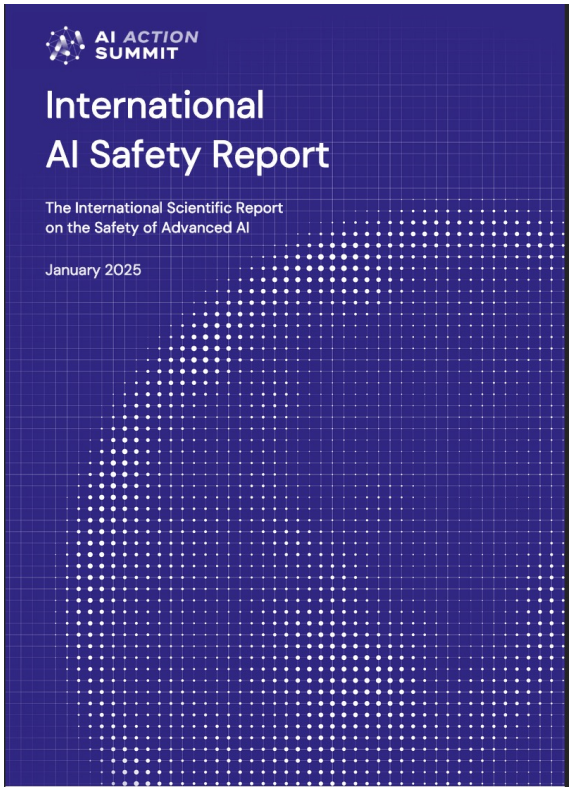
L’adoption de l’IA: nouvelle adaptation coévolutive

Hudhayfa Nazoordeen





Typologie des risques



Risks

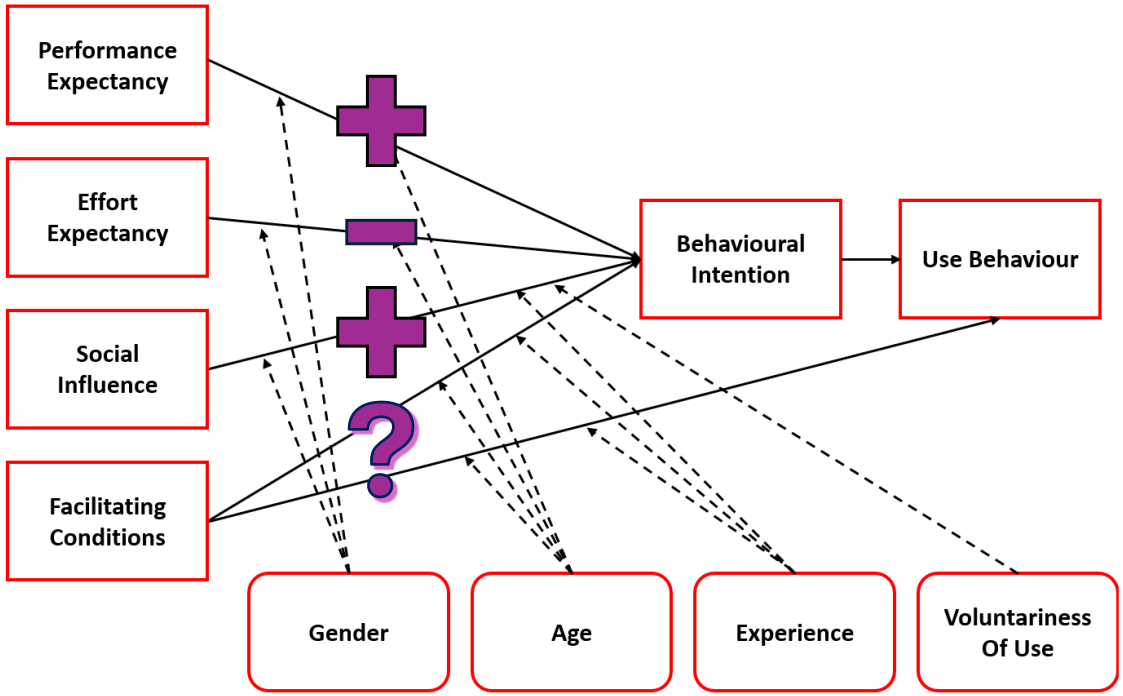
- 2.1. Risks from malicious use
  - 2.1.1. Harm to individuals through fake content
  - 2.1.2. Manipulation of public opinion
  - 2.1.3. Cyber offence
  - 2.1.4. Biological and chemical attacks
- 2.2. Risks from malfunctions
  - 2.2.1. Reliability issues
  - 2.2.2. Bias
  - 2.2.3. Loss of control
- 2.3. Systemic risks
  - 2.3.1. Labour market risks
  - 2.3.2. Global AI R&D divide
  - 2.3.3. Market concentration and single points of failure
  - 2.3.4. Risks to the environment
  - 2.3.5. Risks to privacy
  - 2.3.6. Risks of copyright infringement
- 2.4. Impact of open-weight general-purpose AI models on AI risks

Le panorama des risques selon le NCSC

	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	Moderate uplift	Moderate uplift	Uplift
Social engineering, phishing, passwords	Uplift	Uplift	Significant uplift (from low base)
Tools (malware, exploits)	Realistic possibility of uplift	Minimal uplift	Moderate uplift (from low base)
Lateral movement	Minimal uplift	Minimal uplift	No uplift
Exfiltration	Uplift	Uplift	Uplift
Implications	Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation.	Most capability uplift in reconnaissance, social engineering and exfiltration. Will proliferate AI-enabled tools to novice cyber actors.	Lower barrier to entry to effective and scalable access operations - increasing volume of successful compromise of devices and accounts.

Source: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

Modèle unifié d'acceptation des technologies (Venkatesh et al. 2003)



Appropriation de l'IA par l'écosystème cybercriminel

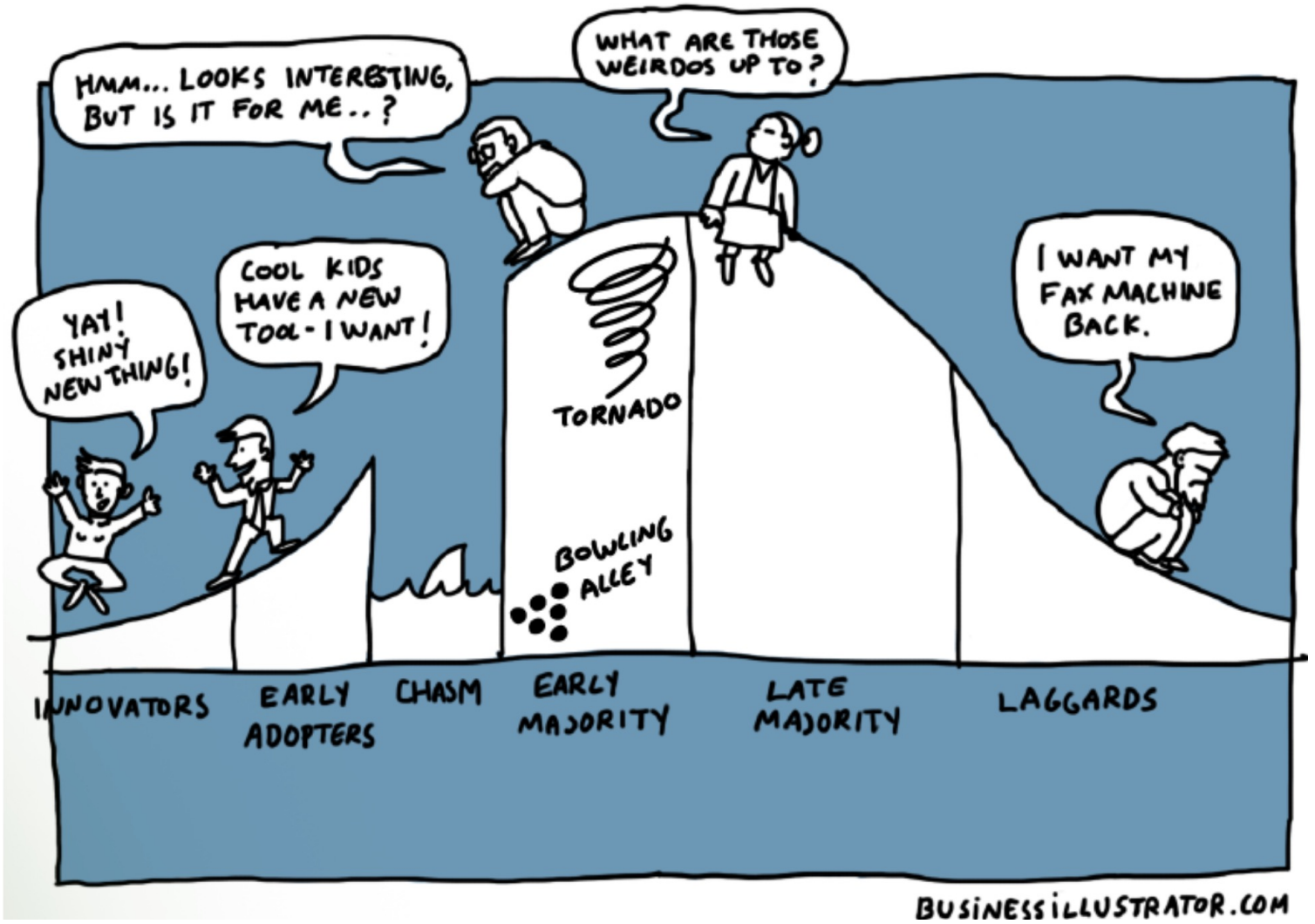
- Accès à un outil qui collecte chaque jour environ:

  3M de messages et posts
  - 164 forums ~ 45k posts par jour
  - 2400 canaux Telegram ~ 2,2M messages par jour
  - 33 marchés clandestins ~ 52k produits et services par jour
  - + Blogs, internet ouvert, sites de rançons, etc.
- Forums: XSS_is, Exploit_in, Dread, BreachForums, darknet_army, turkhackteam, et beaucoup plus.
- Extraction et traduction par un outil d'IA générative (Threat Flow) / 96,22% de précision pour l'extraction des données & 98% pour le résumé

Thèmes émergents

LLM criminels commerciaux	19%
Curiosité	12%
‘Jailbreaking’ de LLMs grand public	12%
Utilisation malveillante de LLMs grand public	10%
Innovations liées aux usages criminels de l’IA	10%
Effets négatifs de l’IA sur l’écosystème cybercriminel (spam, contenus synthétiques)	8%
Comptes GPT hackés	6%
Tutos IA malveillantes	6%
IA et OpSec (contrecarrer la linguistique forensique)	4%

N=47


HMM... LOOKS INTERESTING, BUT IS IT FOR ME..?
WHAT ARE THOSE WEIRDOS UP TO?
YAY! SHINY NEW THING!
COOL KIDS HAVE A NEW TOOL - I WANT!
TORNADO
BOWLING ALLEY
I WANT MY FAX MACHINE BACK.
INNOVATORS
EARLY ADOPTERS
CHASM
EARLY MAJORITY
LATE MAJORITY
LAGGARDS
BUSINESSILLUSTRATOR.COM

Implications pour la recherche et les interventions policières

- Saisir les évolutions de l'écosystème cybercriminel sur une plus longue durée: **temporalité du cybercrime** (pas uniquement compressée, mais aussi étirée > mutations & bifurcations)
- Intégrer les **contraintes, les préférences et les biais** des acteurs cybercriminels dans la modélisation de leur prise de décision (leadership, OpSec, etc.)
- Comprendre et **anticiper les enchaînements** d'interactions probables découlant de certaines interventions
- Possibilité d'un **écosystème cybercriminel multi-espèces** dans lequel des systèmes pourraient agir aux côtés d'humains en disposant néanmoins d'une certaine autonomie ?

Merci!

benoit.dupont@umontreal.ca