Documentation et analyse de la menace
ENSIBS, 2022-2023

Crime et Cyberespace

Une histoire du cyberespace et de ses phénomènes criminels

Ronan Mouchoux
Spécialiste en Analyse de la menace cyber

École d'ingénieurs
ensibs
Université Bretagne Sud

Présentation de l'intervenant

XRATOR
CONQUER YOUR RISK

- *Plateforme de gestion des risques*
- *Services:*
  - *Gestion des risques*
  - *Threat modeling*
  - *VAPT & Red Team*
  - *Conseil stratégique*

École d'ingénieurs ensibs : Université Bretagne Sud

Manager du module « Intelligence Cyber»

ESSEC BUSINESS SCHOOL

Manager externe du module « Security Strategy »

utt UNIVERSITÉ DE TECHNOLOGIE TROYES

Intervenant en analyse de la menace et criminologie numérique

RONINTEL
Cyber Threat Knowledge Management

2019-2021 TAL pour l'analyse de la menace

KASPERSKY lab

2017-2019 Analyse de la menace

SEKOIA

2015-2017 Analyse de la menace

AIRBUS DEFENCE & SPACE

2013-2015 Analyse de la menace

LA POSTE

2008-2013 Réseau & Sécurité

iut Saint Malo réseaux & télécoms

Réseau et Télécom (2008-2010)

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Réseau et Télécom (2010-2013)

le cnam

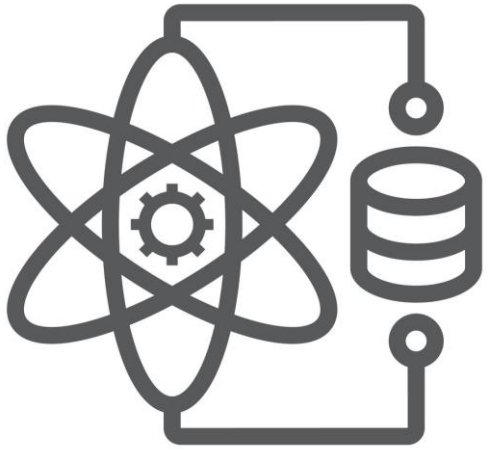
Criminologie (2015-2016)

Sujets d'Intérêts

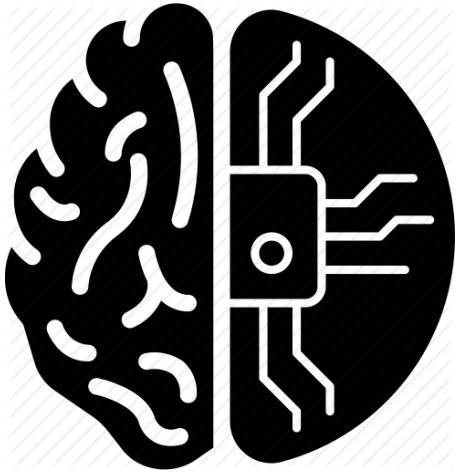
Réseau informatique

Organisation Criminelle

Géopolitique



Théorie de l'Information &
Science de la donnée



Cognition des Humains &
des Automates

Science

Histoire

Philosophie

You don’t have a cyberattack problem…

*… you have an **adversary** problem.*

Vocabulaire

Gestion des risques

Identifier, quantifier, prioriser et minimiser les effets de l'incertitude sur les objectifs.

Une réalisation est remarquable si elle a une chance d'échouer. Il faut donc se préparer.

Cybersécurité

Technologie,processus et pratiques conçues pour réduire la probabilité ou la sévérité d'une cyber attaque.

Construire et entretenir le « Château Fort ».

Cyberdéfence

Personnes, Outils et Processus impliqués dans la réaction et la résistance face aux attaques.

Rassembler, préparer et diriger « l'armée ».

Gouvernance

Le processus de définir les responsabilités et la stratégie pour encourager les comportements désirés.

Construire et superviser la « Chaine de commandement ».

Adversaire / Threat Actor

Individus, Groupes ou Organisations suspectées de conduire des operations criminelles.

Le plan maléfique est au Grand méchant ce que la cyberattaque est à l'Adversaire.

Une histoire du cyberespace

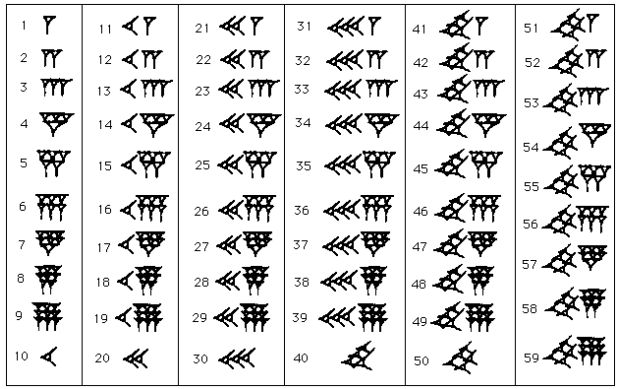
Chaque aventure a son « il était une fois… »

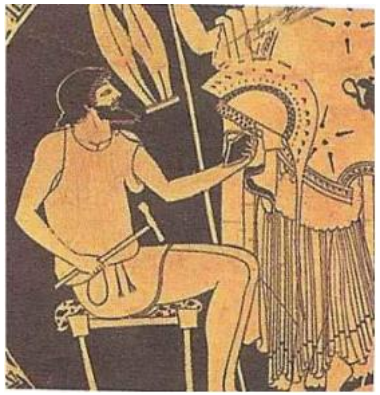
“One of the ways to help make computer science respectable is to show that it is deeply rooted in history, not just a short-lived phenomenon”

Ancient Babylonian Algorithms, Donald E. Knuth, Stanford University (1972)

Du Golem au Cyborg

Depuis la nuit des temps





Algorithme

Depuis (au moins) 3000 AEC

Le concept d'Algorithme est devenu un ***outil analytique*** populaire en historiographie des mathématiques depuis les années 1990. Cela s'est avéré très fructeux pour l'étude des ***mathématiques non occidentales***.

Robotique

Depuis (au moins) 800 AEC

Il [Héphaïstos] était aidé par des servantes en or. Elles ***ressemblaient à des filles vivantes****, possédant un esprit, une intelligence, des cordes vocales et la force. Elles apprirent à travailler par les dieux immortels.*

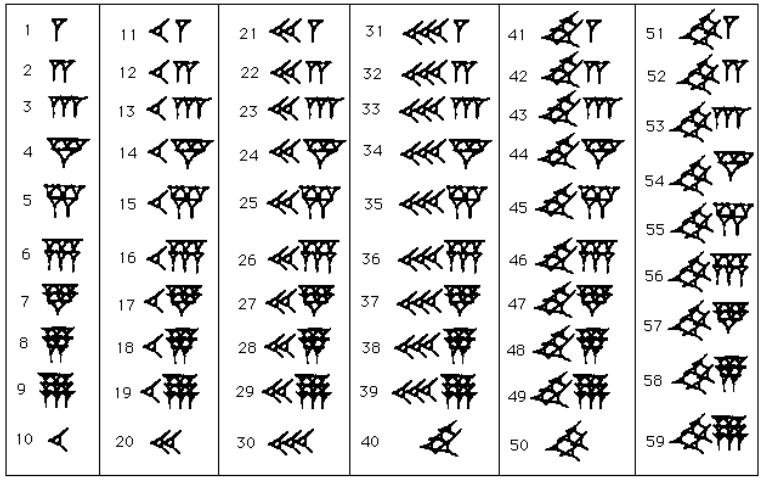
Cybernetique

Depuis (au moins) 380 AEC

Platon utilisait le mot "Kybernytiky" dans ses dialogues "d'Alcibiades" et dans "Gorgias", signifiant "l'art de gouverner un navire", dans "Clitophon", signifiant "l'art de gouverner les hommes" et dans "La Republique", signifiant "***l'art de gouverner,*** en general"

Algorithmes

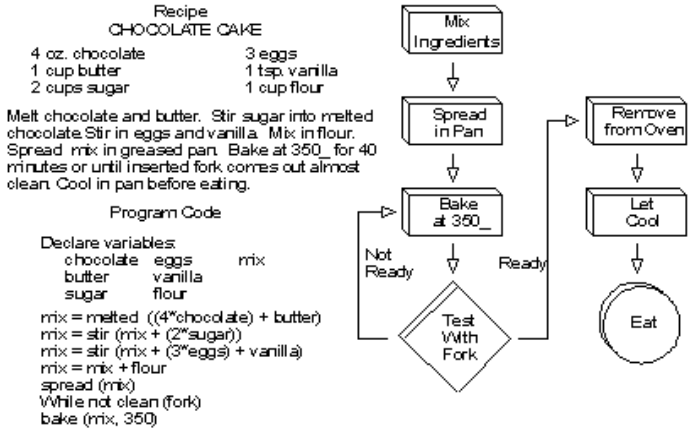
Un algorithme est une ***séquence d'étapes pour réaliser une tâche***. Elle doit être finie, efficace et non ambigue.

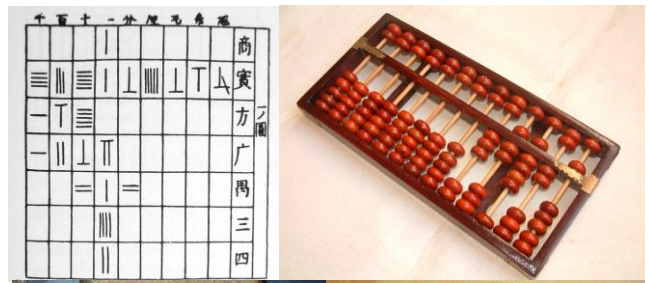


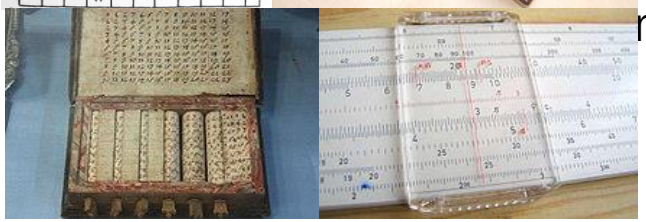
<u>Le système sexagécimal babylonien</u>

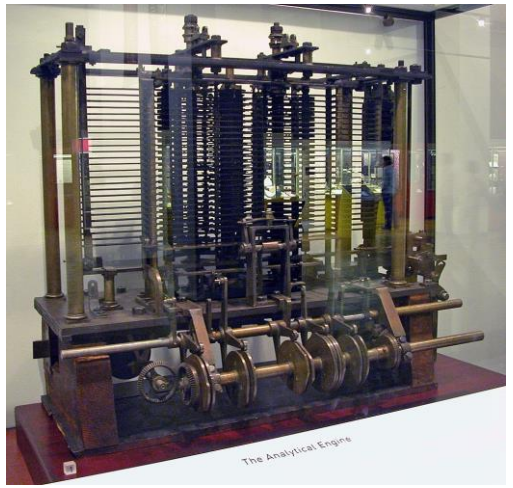
Ils possédait des mathématiques avancées :

- Racine carrée et cubique
- Connaissance de Pi
- Connaissance de l'exponentiel et du logarithme







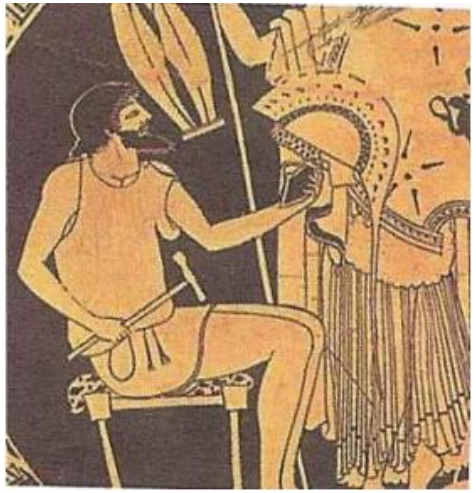


<u>La machine de Babbage (1837)</u>

Première machine à calculer avec une mémoire: « *Et si une machine à calculer pouvait non seulement prévoir, mais agir sur cette prévision*.»

Robotique et Intelligence Artificielle

Il y a "*Intelligence Artificielle*" dès qu'un processus est ***dépersonnalisé par un système*.**

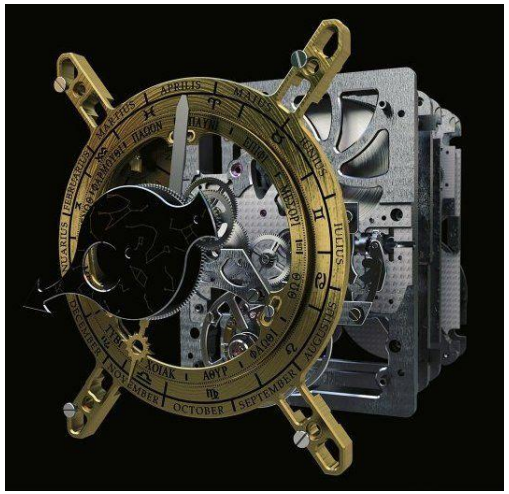


Les servantes d'Hephaïstos

Livre XVIII, Iliade, Homer, 800 AEC

Golem Hébreux

Culture hébraïque, 500 AEC

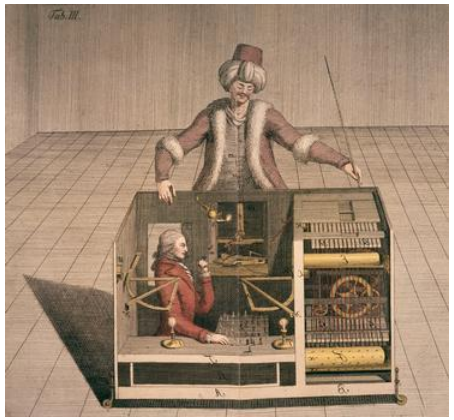


Machine d'Anticythère

Scientifique grecs, 205 AEC – 90 AEC

Objets Vivants Fous

Le Menteur, Lucien de Samosate (120 AEC)



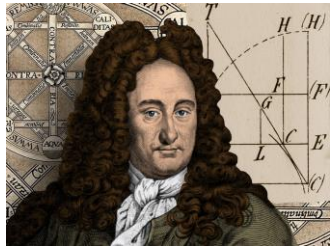
Le Turc Mécanique

Wolfgang von Kempelen, 1854

Robots et Cyborgs

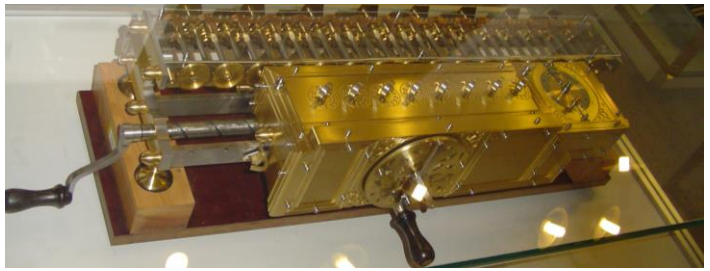
Rossum's Universal Robots, Karel Čapek, 1920

Robotique et Intelligence Artificielle



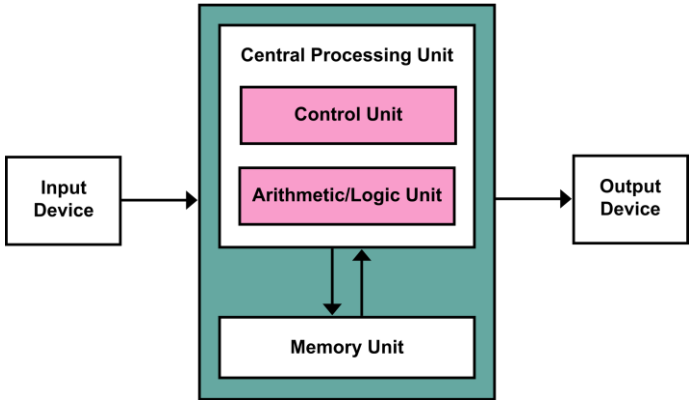
Calculus Ratiocinator de Leibniz (1666)

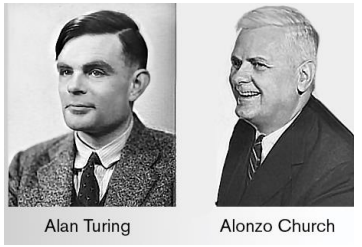
- Un algorithme basé sur un langage universel (*Characteristica Universalis*) capable d'identifier le vrai du faux dans une discussion.
- L'externalisation du potentiel humain de raisonnement formel et logique par une machine programmable.
- Deux concepts :
  - Vue synthétique ("hardware") : la machine à calculer
  - Vue analytique ("software") : le moteur d'inférence



Architecture de Von Neumann (1945)

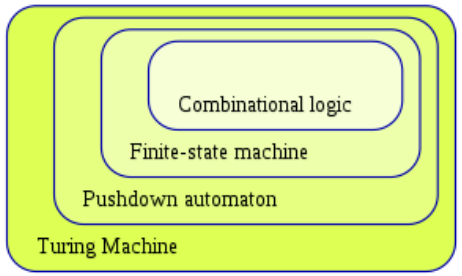
- Architecture d'un ordinateur numérique
- Cinq composants basiques
  - *Un processeur (logique arithmétique et mémoire court terme)*
  - *Une unité de contrôle (gestion des instructions)*
  - *Une mémoire (stockage des données et instructions)*
  - *Un stockage externe*
  - *Une gestion des flux d'entrées/sorties*





Thèse Church-Turing (1952)

- Une hypothèse sur l'informatisation de toute fonction mathématique en utilisant une machine de Turing et le système binaire.
- La machine de Turing est un modèle abstrait formalisant une procedure mécanique.
- Turing était convaincu que ***la cognition humaine est un ensemble de calculs qui peut être traité par une machine.***



Interlude : Robotics & Artificial Intelligence

A very comprehensive and precise spec, CommitStrip, 2016-08-25
http://www.commitstrip.com/en/2016/08/25/a-very-comprehensive-and-precise-spec/

Cybernetique

Platon, La Republique (382 AEC) et le Gorgias (390 AEC)

La cybernetique (κυβερνητικη) est la science du gouvernement.

La cybernétique platonicienne est basée sur la métaphore du gouvernail d'un navire. Il compare la réalisation de tout processus orienté action avec la trajectoire d'un navire effective, la trajectoire souhaitée, et la rétro-action à l'œuvre.

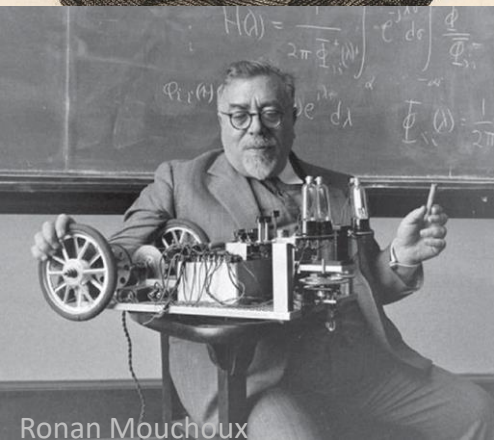
Philosophie pythagorienne
« Tout est chiffre»

André Marie Ampère, Essaie sur la philosophie des sciences, Tome 2 (1843)

La cybernétique est une « *Science du troisième ordre sur les moyens par lesquels les gouvernements assure la sécurité extérieur et assure l'ordre et la paix au sein de leur territoire.*»

Philosophie newtonienne
« Tout est déterministe »

La cybernétique ampérienne désigne la connaissance de toute ce qui constitute une nation et de tous les principes par lesquels les dirigeants prennent des decisions pour gérer une situation.



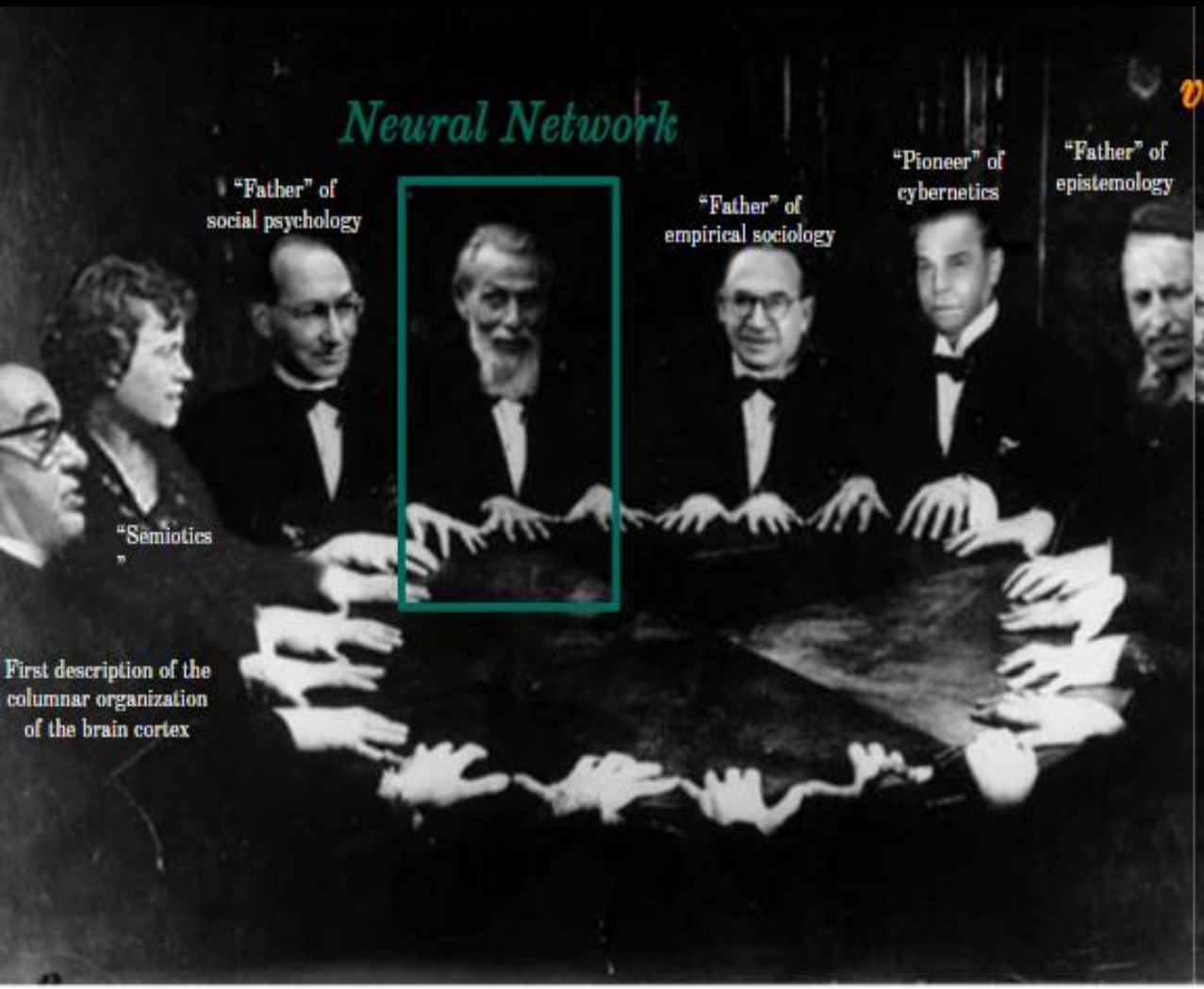
Norbert Wiener et les "Conférences de Macy"

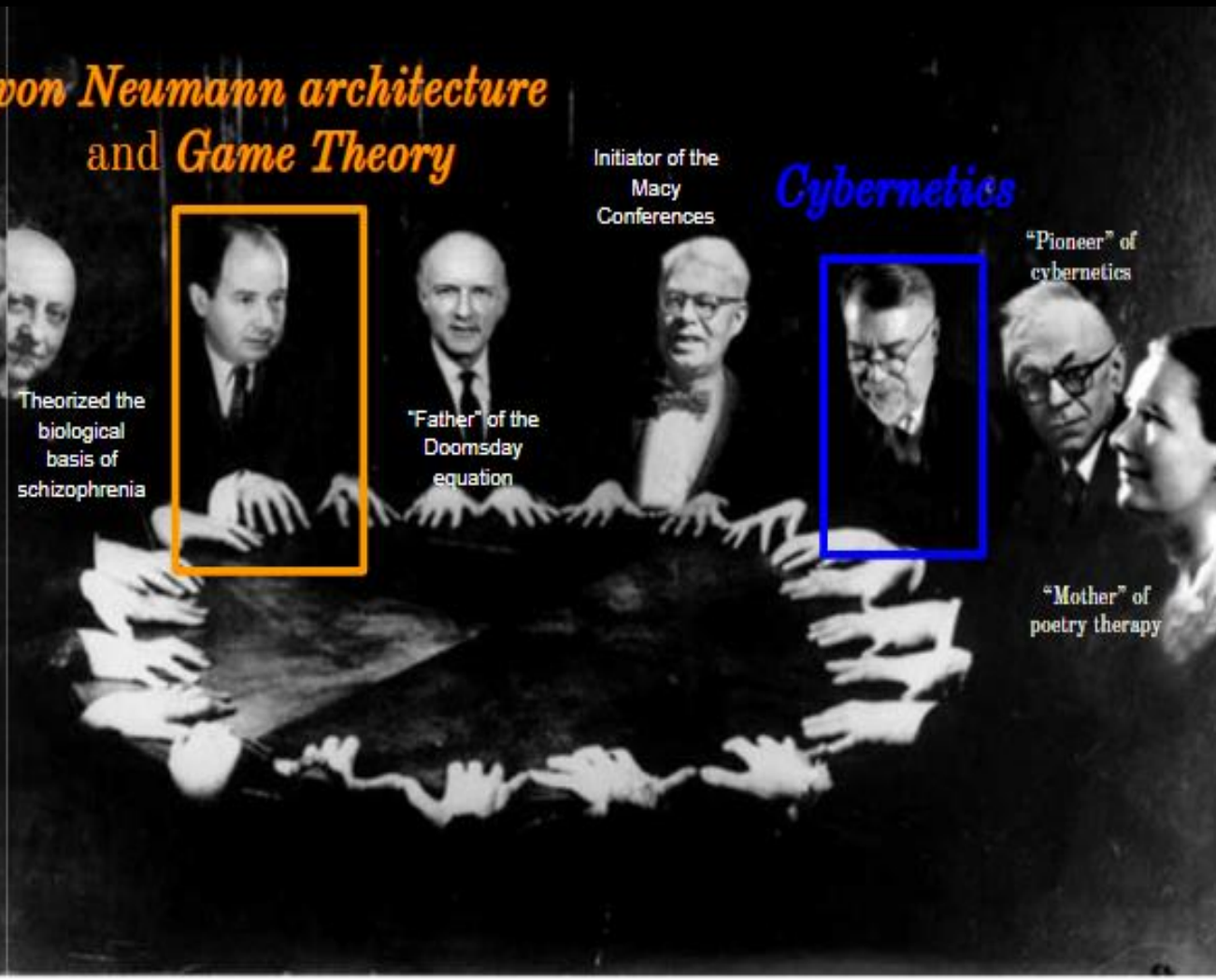
1948 – Cybernetics, or Control and Communication in the Animal and the Machine
1950 – Cybernetics and Society : The Human Use of Human Being

Philosophie quantique
« Tout est probabiliste»

La cybernétique wienerienne est l'étude scientifique des échanges d'informations pour le contrôle des animaux et des machines.

Cybernétique et Conférence de Macy (1941-1960)

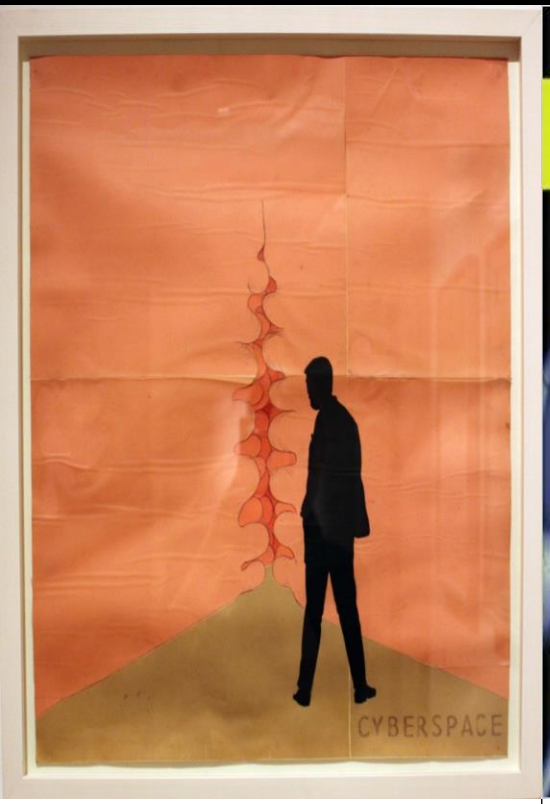




Cybernetic Séance - New York City, 1947
From Left to Right : Rafael Lorente De No (Neurophysiologist), Margaret Mead (Anthropologist), Kurt Lewin (Psychologist), Warren S. McCulloch (Neuropsychiatrist), Paul F. Lazarsfeld (Sociologist), Arturo Rosenblueth (Physiologist) and Gregory Bateson (Anthropologist). Front (missing from view): Molly Harrower (Psychologist), Heinrich Klüver (Psychologist), Norbert Wiener (Mathematician), Lawrence K. Frank (Social Scientist), Heinz von Foerster (Electrical Engineer), John von Neumann (Mathematician) and Ralph W. Gerard (Neurophysiologist). Observers (missing from view): Frank Fremont-Smith (Medical Director of the Macy Foundation), Julian Bigelow (Computer Engineer), Walter Pitts (Mathematician), George Evelyn Hutchinson (Ecologist), Leonard J. Savage (Mathematician), Henry Brosin (Psychiatrist), Theodore Schneirla (Comparative Psychologist), Hans Lukas Teuber (Psychologist), Gerhardt von Bonin (Neuroanatomist), Lawrence S. Kubie (Psychiatrist), Filmer S. C. Northrop (Philosopher), Alex Bavelas (Social Psychologist) and Donald Marquis (Psychologist).

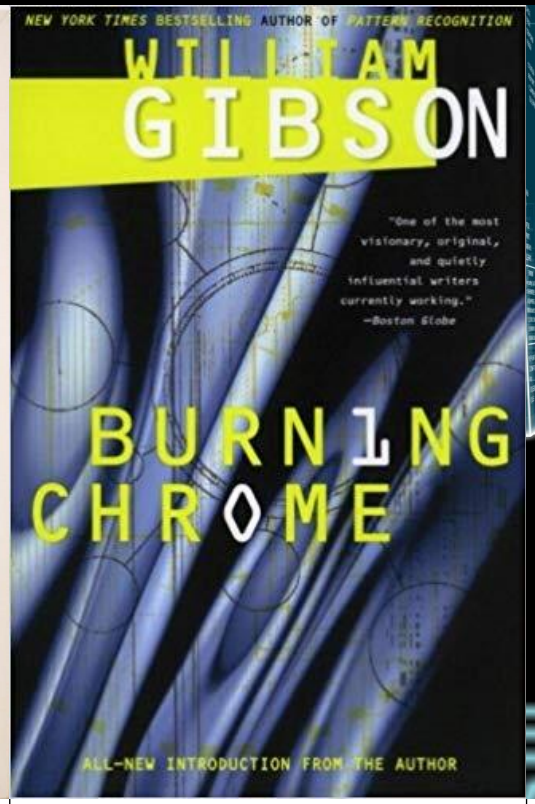
Cybernetic Séance - New York City, 1947
From Left to Right : Ralph W. Gerard (Neurophysiologist), John von Neumann (Mathematician), Heinz von Foerster (Electrical Engineer), Lawrence K. Frank (Social Scientist), Norbert Wiener (Mathematician), Heinrich Klüver (Psychologist), Molly Harrower (Psychologist). Front (missing from view): Rafael Lorente De No (Neurophysiologist), Margaret Mead (Anthropologist), Kurt Lewin (Psychologist), Warren S. McCulloch (Neuropsychiatrist), Paul F. Lazarsfeld (Sociologist), Arturo Rosenblueth (Physiologist), Gregory Bateson (Anthropologist). Observers (missing from view): Frank Fremont-Smith (Medical Director of the Macy Foundation), Julian Bigelow (Computer Engineer), Walter Pitts (Mathematician), George Evelyn Hutchinson (Ecologist), Leonard J. Savage (Mathematician), Henry Brosin (Psychiatrist), Theodore Schneirla (Comparative Psychologist), Hans Lukas Teuber (Psychologist), Gerhardt von Bonin (Neuroanatomist), Lawrence S. Kubie (Psychiatrist), Filmer S. C. Northrop (Philosopher), Alex Bavelas (Social Psychologist) and Donald Marquis (Psychologist).

Cyberespace – une origine artistique



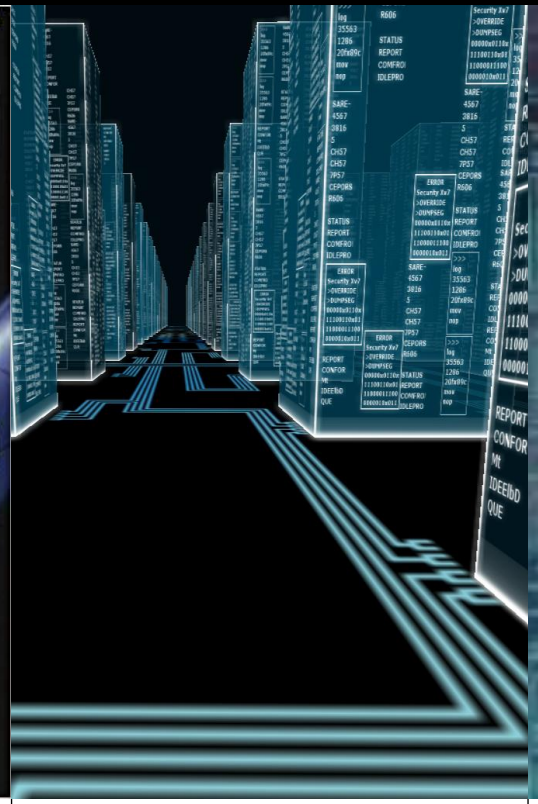
Cyberspace,
Susanne Ussing, 1968

« Gestion de l'espace»



Burning Chrome,
William Gibson, 1982

« Une représentation graphique de la donnée abstraite et de leurs banques de tous les ordinateurs du système humain.»

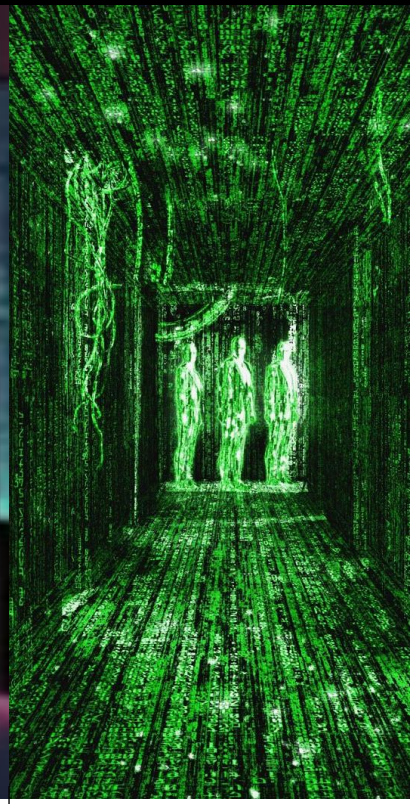


Tron,
1982

« Monde physico-virtuel»

Hackers,
1995

« Représentation graphique abstraite de la données et des Mainframes»

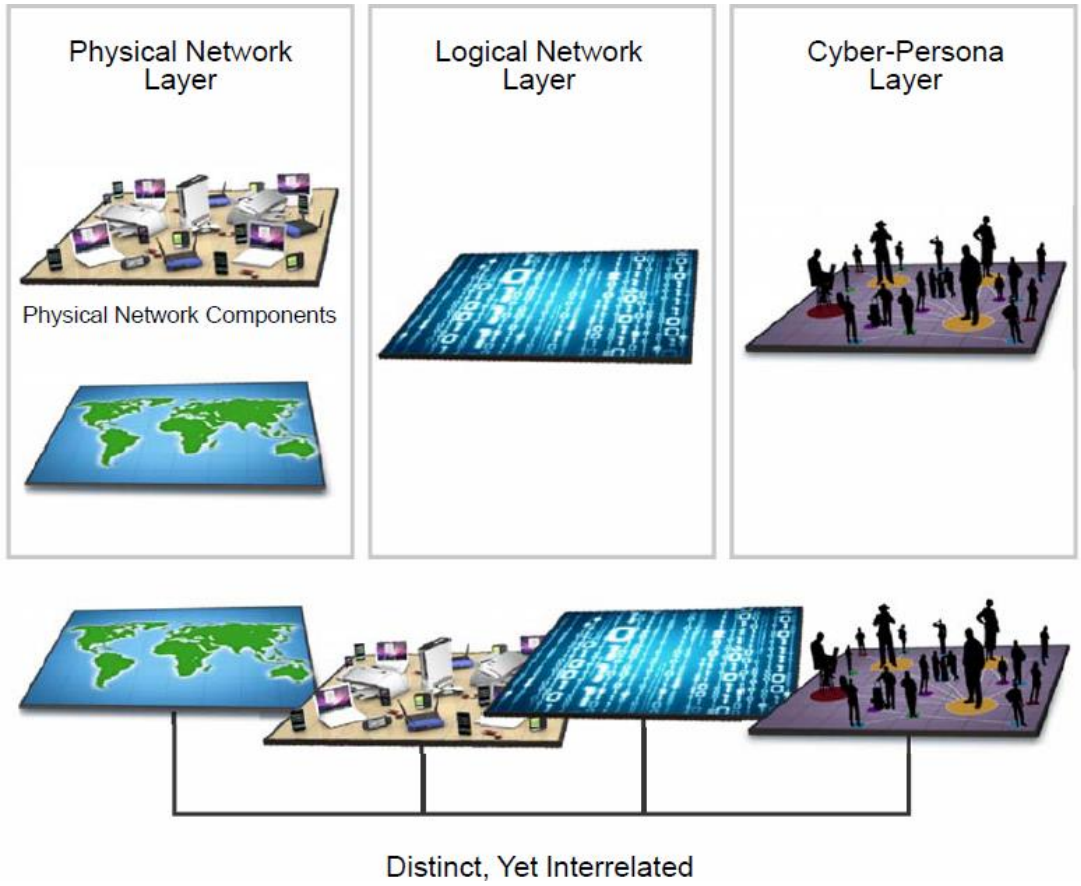


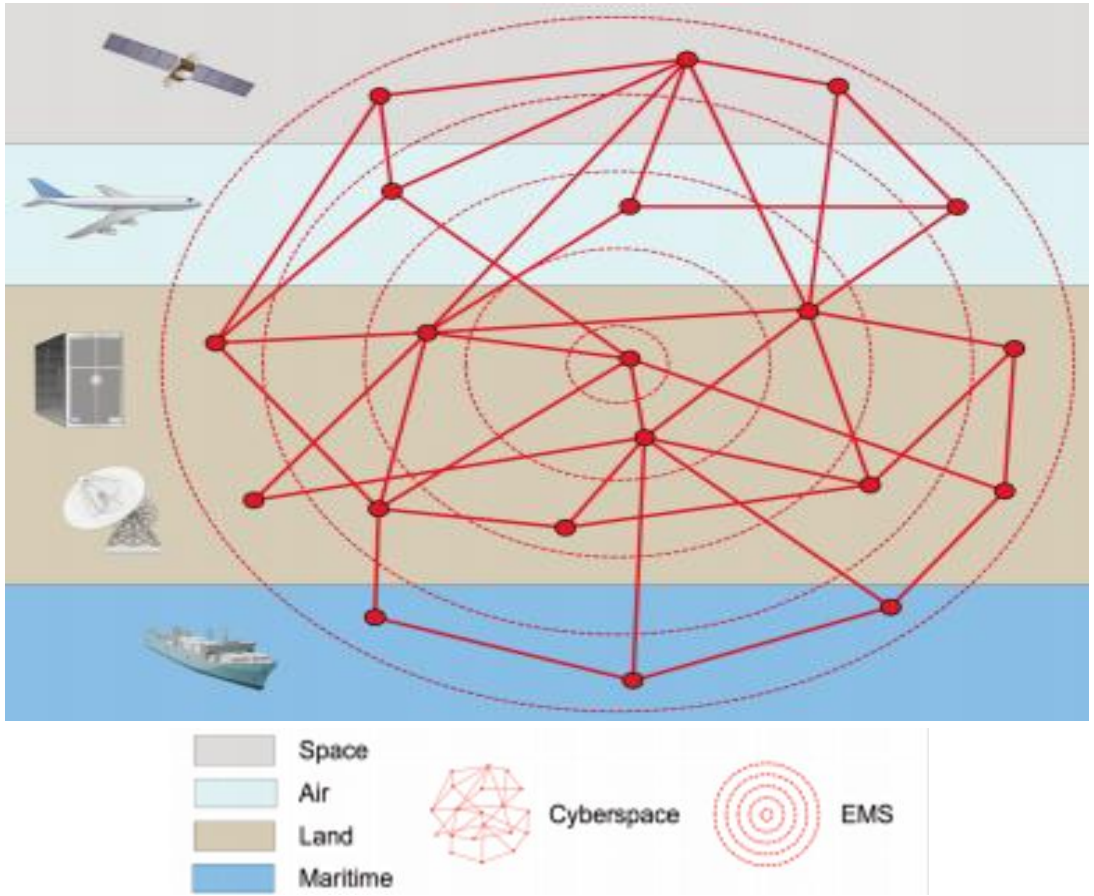
Matrix,
1999

« Monde physico-virtuel»

Cyberespace – Une formalisation militaire

Le Cyberespace est un ***domaine global et dynamique***. Il repose sur les électrons, les photons et le spectre électromagnétique pour créer, stocker, modifier, échanger, monétiser, extraire, utilizer et détruire des informations; et pour intéragir avec le monde physique.



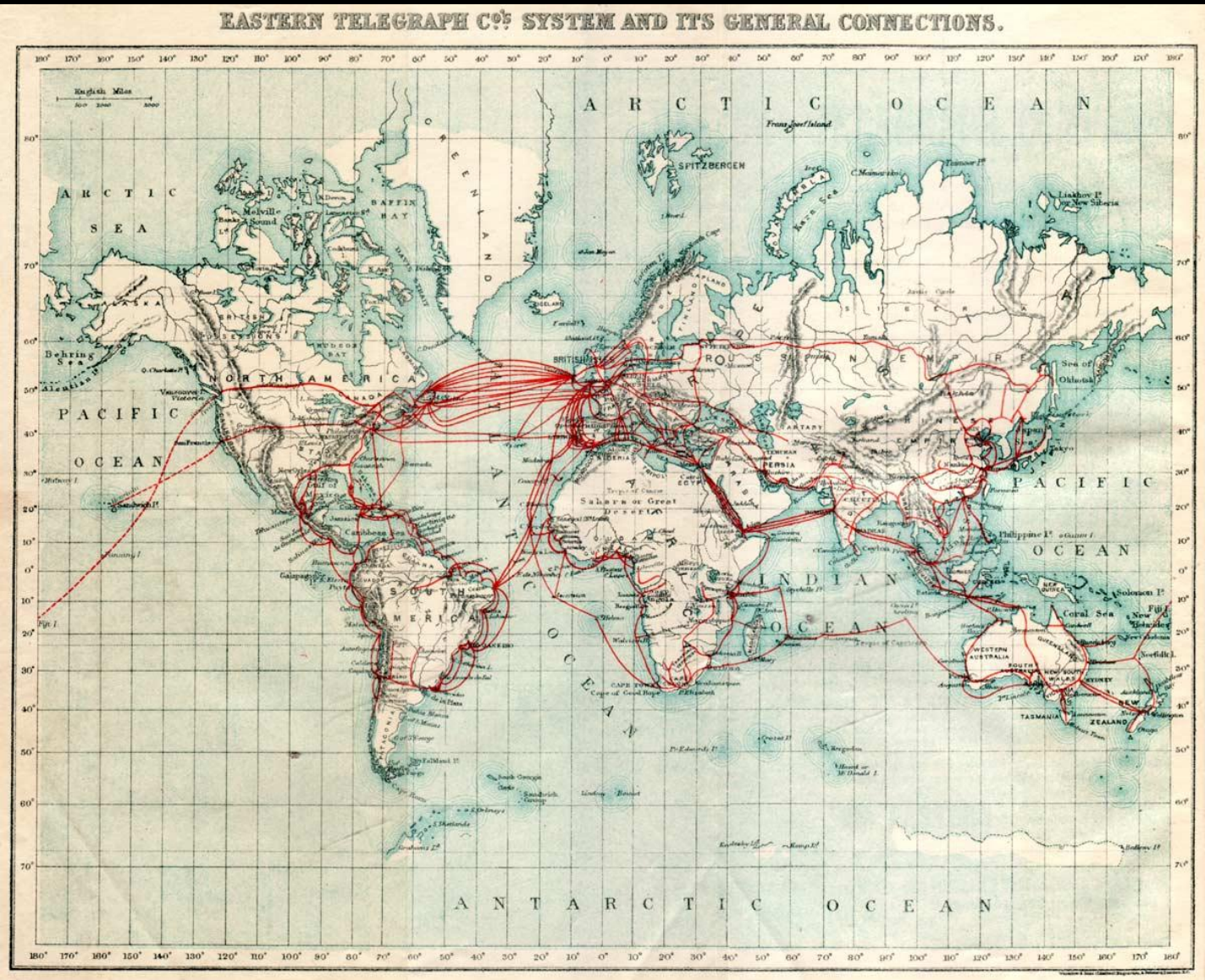


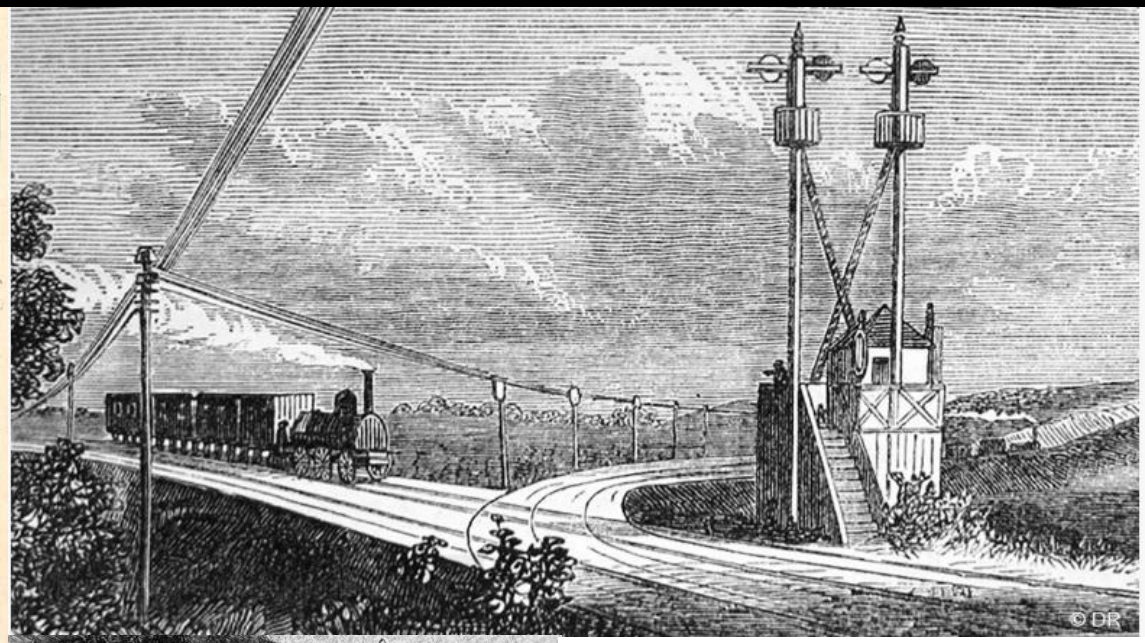
"*Cyberpower and National Security: Policy Recommendations for a Strategic Framework*", Cyberpower and National Security, National Defense University Press, 2009

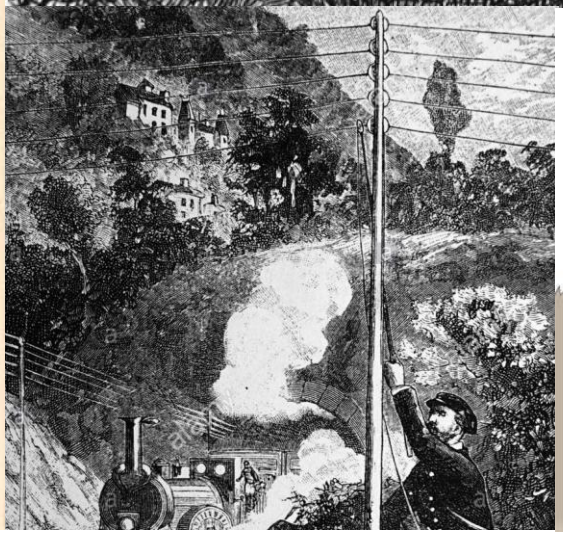
&

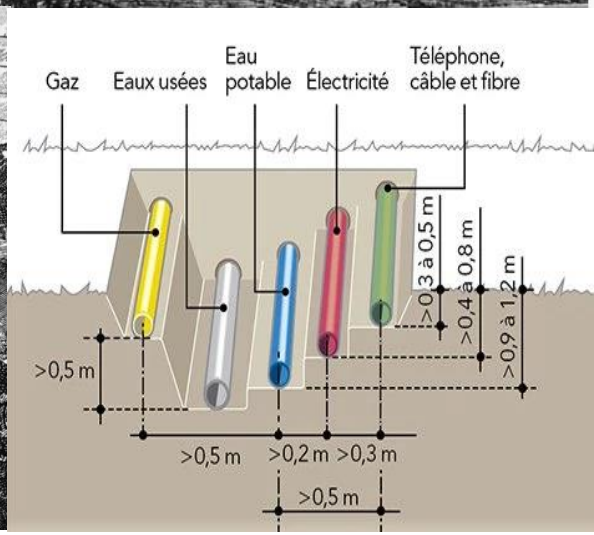
Joint Publication 3-12 Cyberspace Operations, US Army

Cyberespace et Transhumances Humaines





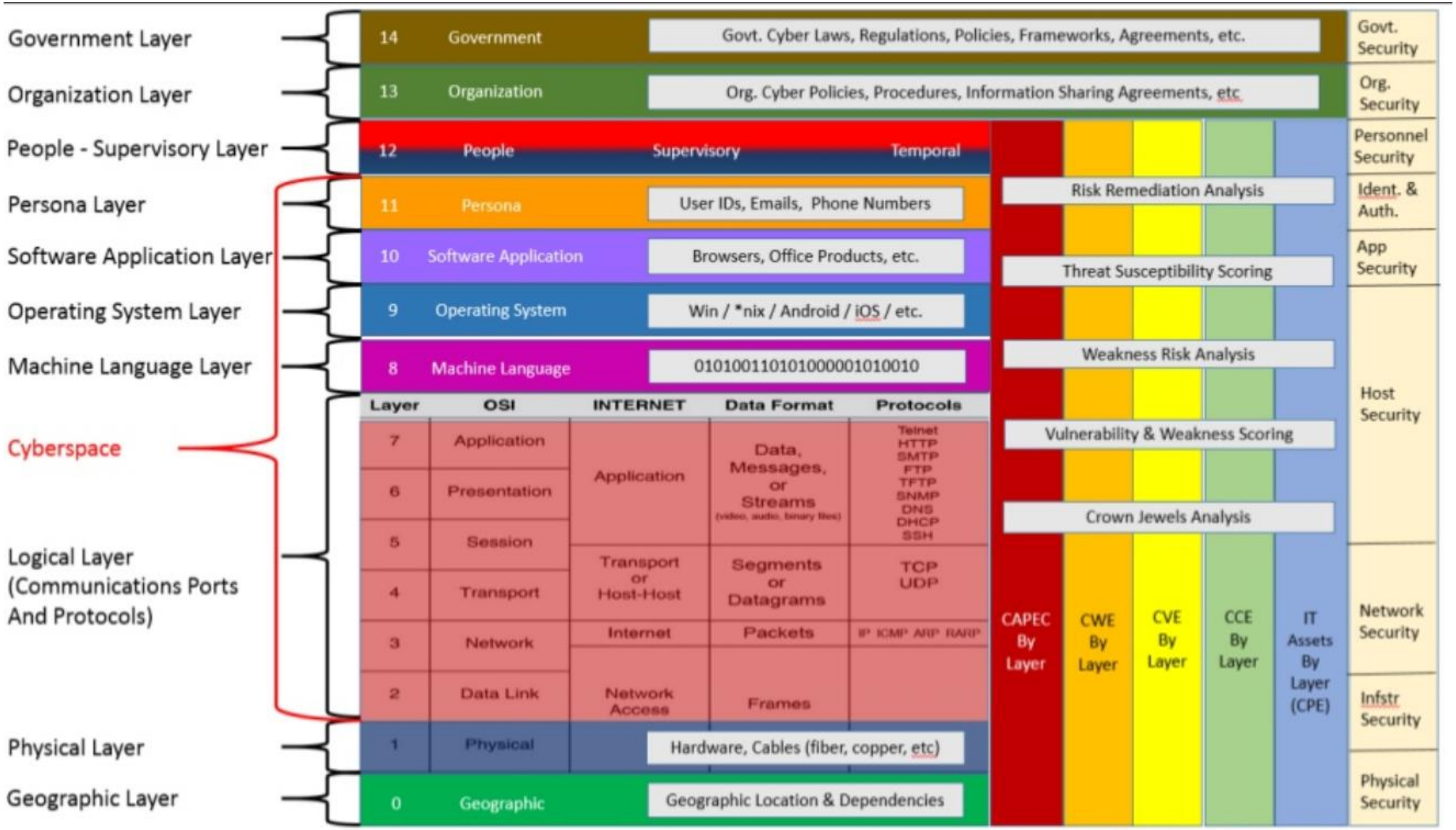




Eastern Telegraph Company System Map (1901) : http://www.visualcomplexity.com/vc/project.cfm?id=373

L'intrusion du télégraphe electrique dans les chemins de fer : https://www.railpassion.fr/histoire/lintrusion-telegraphe-electrique-chemins-de-fer/

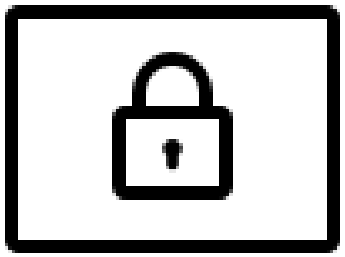
The Cyber Sandwich



Science of Security: Cyber Ecosystem Attack Analysis Methodology -> https://www.slideshare.net/shawnriley2/cs1-2-riley

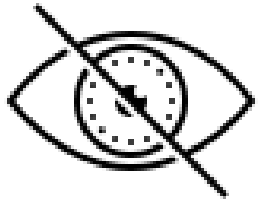
Interlude : le plan des Cypherpunks

Dans les années 1980, un groupe d'activiste libertaire du monde entire (principalement USA) travaillent à protéger la vie privée en ligne des humains face à des gouvernements et entreprises prédatrices, grâce à un usage systématique et proactive de la cryptographie : les ***cypherpunks***.



Confidentialité
Un message ne peut être lu que par son destinataire.

Authentification
Une prevue qu'une personne est bien celle qu'elle declare être.



Anonymat
La possibilité de cacher son identité réelle grâce à des mandataires ("proxy").

Monnaie Intraçable
La possibilité d'acheter quelque chose sans trace ("e-cash").

Transaction cachée
La possibilité pour un vendeur et un acheteur d'agir sans trace.

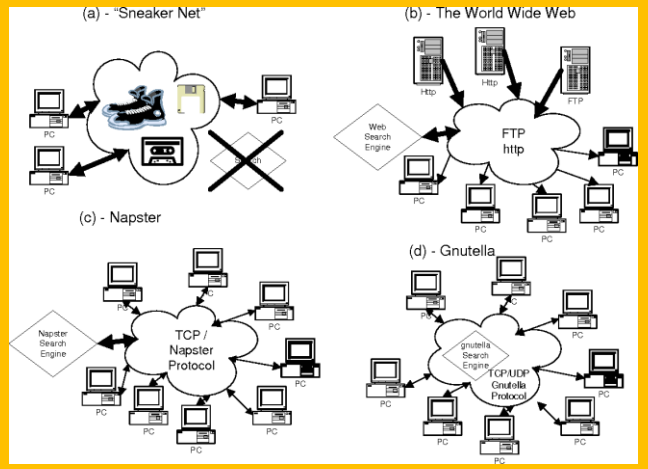
https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085

Interlude : l'héritage Cypherpunks

Les reseaux informatiques superposés distribués (généralement appelé "***Darknets***")
suivent une implementation graduelle du cahier des charges cypherpunk.

1ère Génération de Darknets (1990's)

(Disponibilité/Résilience)



KaZaA napster

2ème Génération de Darknets (2000's)

(Confidentialité/Anonymat)

Freenet, Ian Clarke (2000)
P2P Distributed File System
« Small World » Routing
https://freenetproject.org/fr/pages/about.html

I2P, Collective (2003)
Encrypted P2P Network
« Garlic» Routing
https://geti2p.net/fr/comparison/tor

Tor, Tor Project (2003)
Proxy+SSL+P2P+Web
« Onion» Routing
https://www.torproject.org/about/sponsors/

3ème Génération de Darknets (2010's)

(Intégrité/Authenticité)

1ère Génération de Blockchain
Ledger and Transaction System
Ex : Bitcoin (2008)

2ème Génération de Blockchain
Code-based Contract
Ex : Ethereum (2014)

3ème Génération de Blockchain
Interoperable Ledger
Ex : IOTA (2017)

“[In 1950] cybernetics was a relatively new idea, and neither the scientific nor the social implications had become fully clear.

Now [...] the problem of unemployment arising for automatization is no longer conjectural, but has become a very vital difficulty of modern society.”

God and Golem Inc, Norbert Wiener (1964)

Hacking et Piratage du XIXème siècle à aujourd'hui

Ronan Mouchoux

École d'ingénieurs
ensibs
Université Bretagne Sud

1860's : Electronic Warfare

Eletronic Warfare is any action involving the use of the Electro-Magnetic Spectrum (EMS) or directed energy (DEW) to disrupt the adversary's spectrum, disrupt an adversary assault or attack an adversary.

Among the first registered Electronic Warfare stands the ***American Civil War*** (1861-1865) :

- Telegraphic lines were prioritary targets of specialized cavalry units
- These units were tasked to interception, alterate and deny adversary's telecommunications (« MITM »)
- It is estimated that the Union forces, more teleconnected than Confederates, were more vulnerable to these attacks

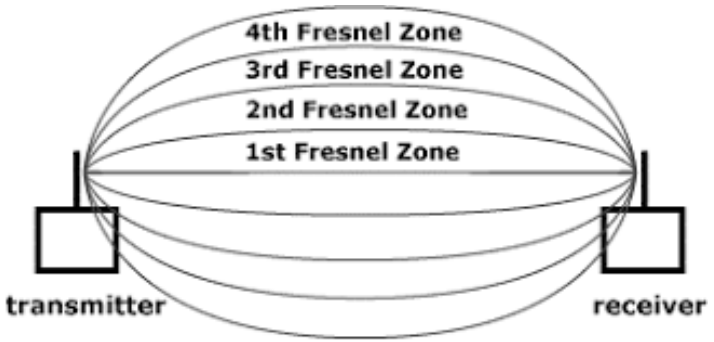
"The evolution of electronic warfare equipment and techniques in the USA, 1901 to 1945
https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/7410/2/353424.pdf

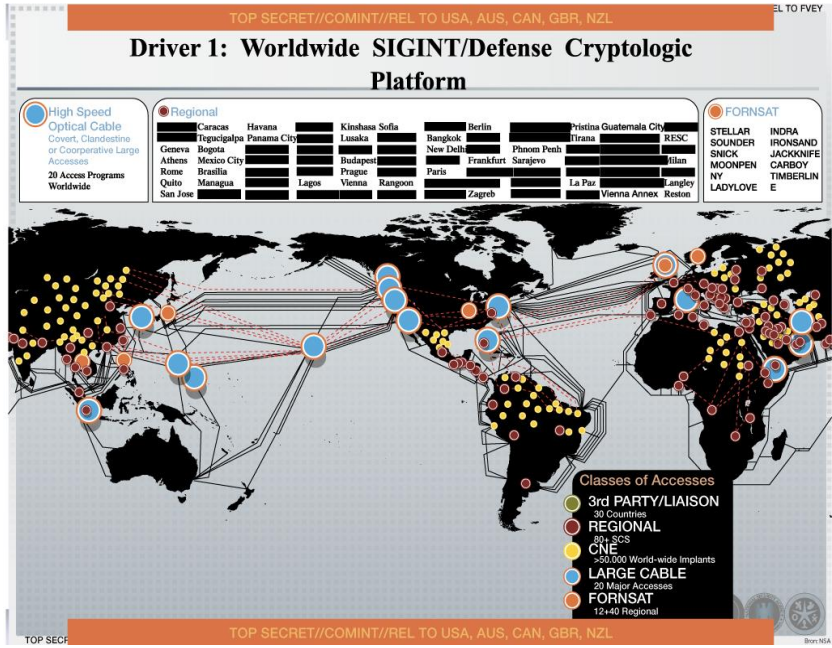
1900's : Signal Intelligence (SIGINT)

Signal Intelligence is the gathering of electro-magnetic signals emitted by human telecommunication (COMINT) or indirectly emitted by human behaviour (ELINT).

Among the first registered Signal Intelligence Operation stands the ***Russo Japanese War*** (1904-1905) :

- British and Italian Navy used the Marconi Radio System whereas French and Russian Navy used the Ducretet Radio System
- The British did already experienced teleconnected battles (Second Boers War) and knew its game changing power
- The British and the Japanese had the idea to gathered and listen to Russian Navy telecommunication over the air



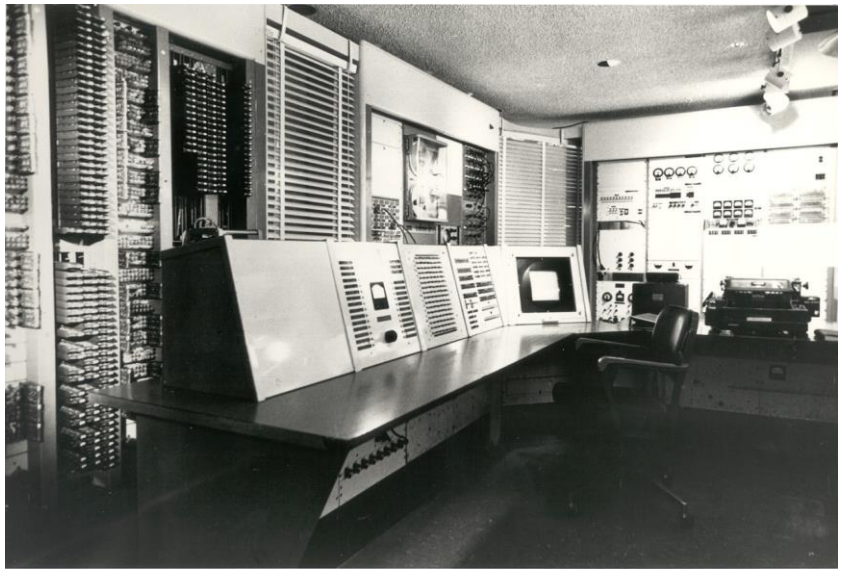


1950's – 1970's : Hacking, a university hobby

Hacking comes from its original meaning : to cut up roughly, as with an axe or a hatchet. MIT Students *hacked* complex systems and problems into smaller pieces, more understandable, to study and modify the complex system behaviour. It became a synonym of *harmless prank* or *tricks* on the campus. A hack was a smart, quick and dirty fix or solution to a problem.

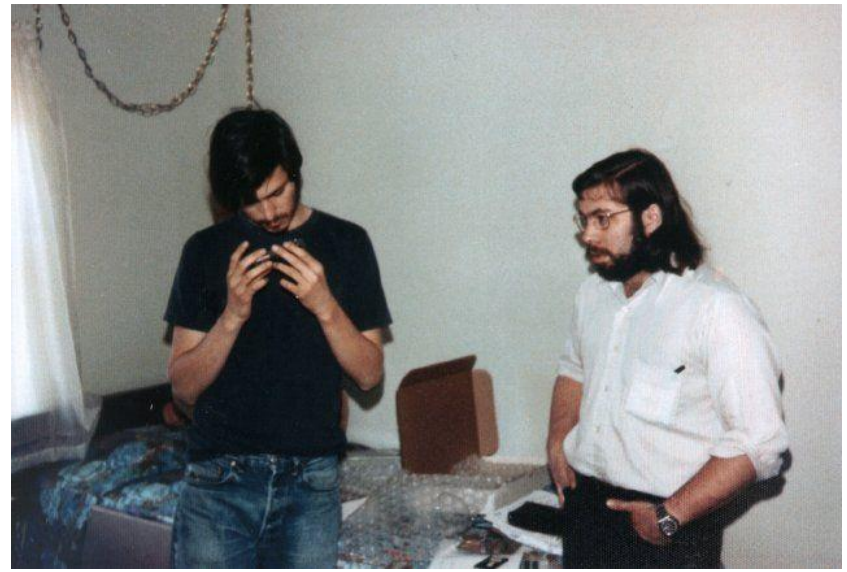
This technological exploratory mentality expands to cryptology, debugging, ***phreaking***. The nerd and self-sufficient stereotype rose, as these systems took times to dig into and the problems made no sense for the general population.

Personal Crime were mainly composed of phreaking (wire bill evasion). In 1966 the first ***corporate computer crime*** was prosecuted, perpetrated by programmer Milo Arthur Bennett.



MIT's first computer

MIT's Tech Model Railroad Club (TMRC)



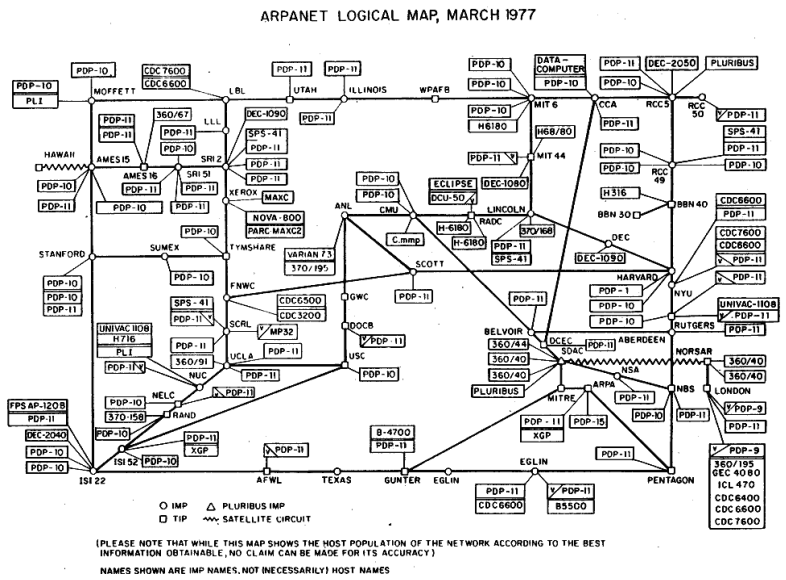
Jobs and Wozniak first product : the phreaking blue blox

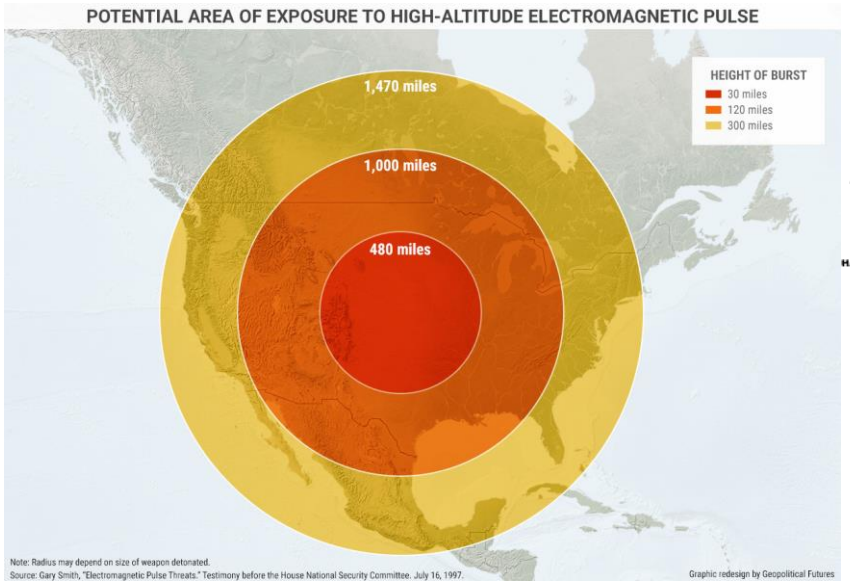
http://tmrc.mit.edu/hackers-ref.html
https://handbook.mit.edu/hacking
http://content.time.com/time/subscriber/article/0,33009,906731,00.html

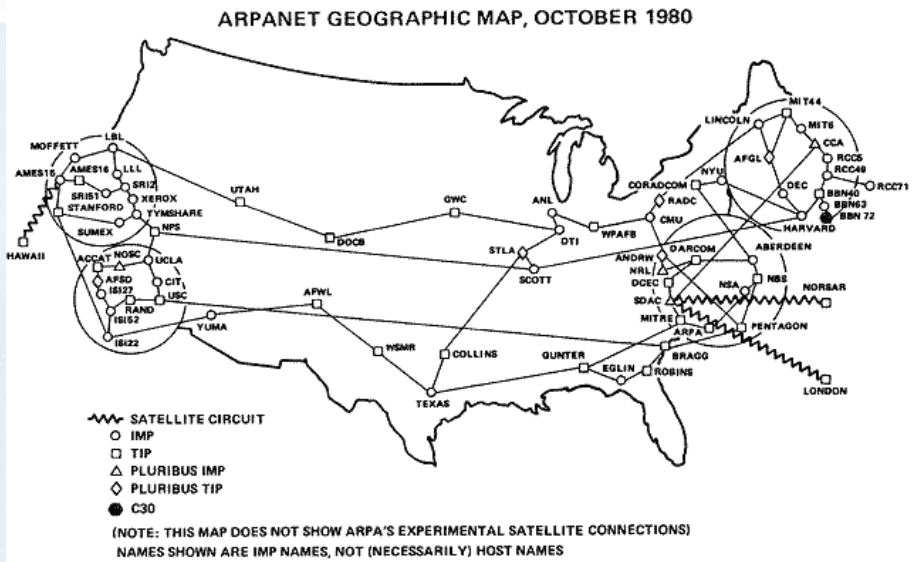
1970's : Drop Ya' Bomb

The Cold Nuclear War was not only a concern for explosion damages and radiation, but also for the Electro-Magnetic perturbation a detonation would bring. As most communications were still signals over-the-air, it has to find a way to increase the usage of underground shielded cables to transmit any kind of data. Here comes the ARPANET (USA), Cyclades (France) or the EIN (Europe).

Probably inspired by the first theorical Computer Worm created by Von Neumann in 1949, ARPA's researcher Ray Tomlinson created the first functional Computer Worm in 1971, ***Creeper***, propagated in the ARPANET. The year later, he created the first Anti-Virus software, ***Reaper***, that was also a Computer Worm but design to track and delete Creeper.







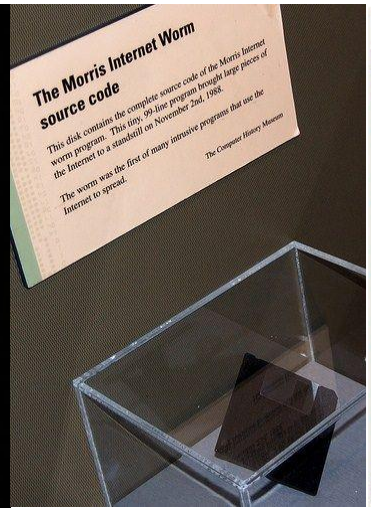
Theory of self-reproducing automata, John von Neumann (1966) : https://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf

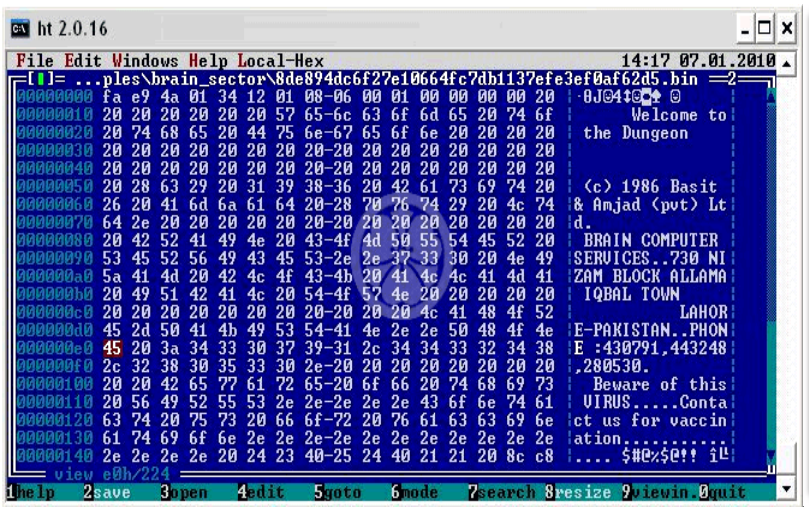
1980's : The Golden Age

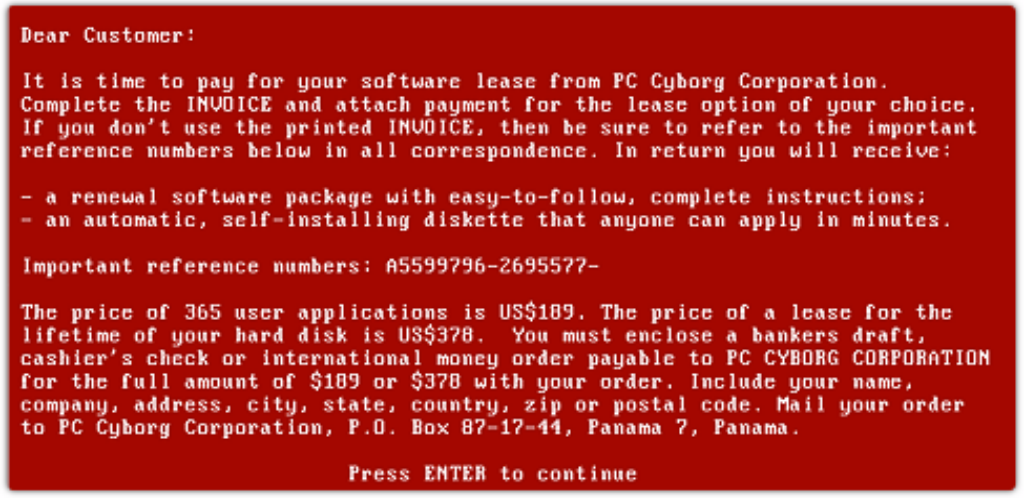
In the 1980's, ***Personnal Computer*** became available in the public. They were less rigid that Sun's or IBM's super computer. It made computer crime more attractive, as it was easier to program virus and there was an increasing connected victims potential.

As soon as 1986, the USA enacted the ***Computer Fraud and Abuse Act*** (CFAA) to amend the Crime Control Act of 1984, in reaction to concern triggered by the WarGames movie (1983), "*a realistic representation of the automatic dialing and access capabilities of the personal computer.*" Previously these crimes were prosecuted as mail and wire frauds.

Notable Malicious Softwares were the Internet Worm Morris, the Arpanet Virus BRAIN and the ransomware PC Cyborg (AIDS Virus). It was also the time of the Kevin Mitnick *hack n' run* adventure (cf the movie Track Down (2000)).



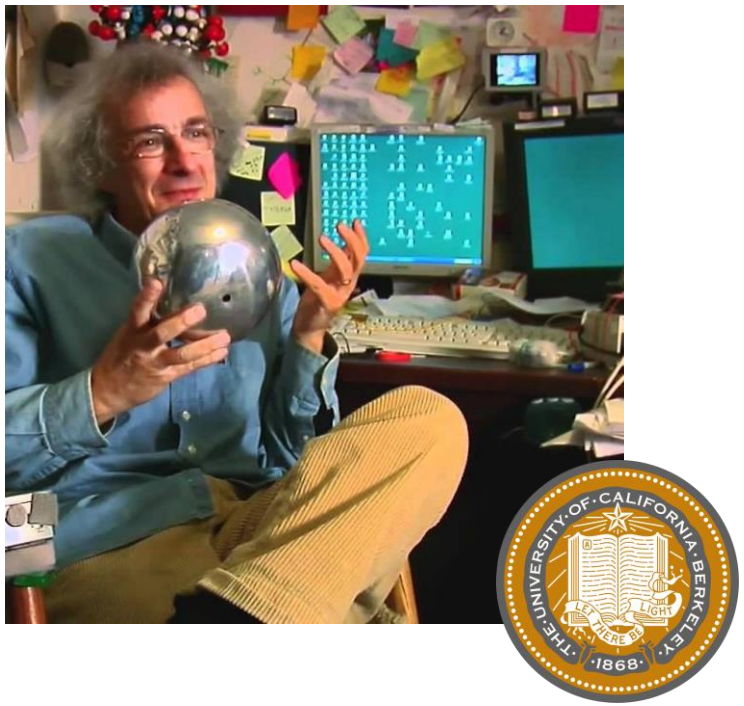


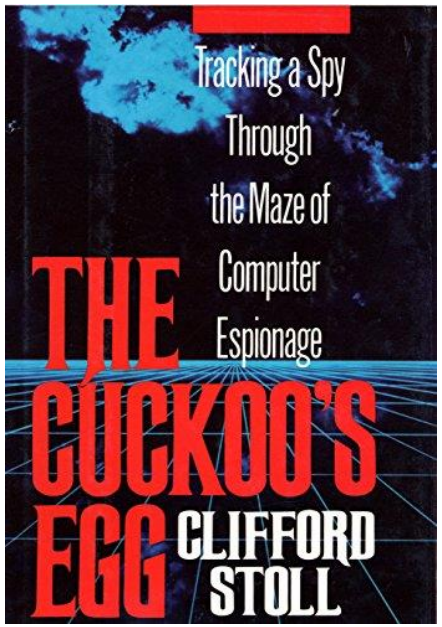


https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf
https://www.f-secure.com/v-descs/brain.shtml

1986 : the first Advanced Targeted Attack Analysis

In 1986, the astrophysicist Dr. Clifford Stoll (Berkeley), then PhD student, detect, analyze and document for the very first time a targeted espionage attack in a computer network. During its investigation, he creates what became the first "***Honeypot***". The attack was performed by Markus Heese, a german citizen selling the stolen information to the soviet KGB ("*Operation Showerhead*").





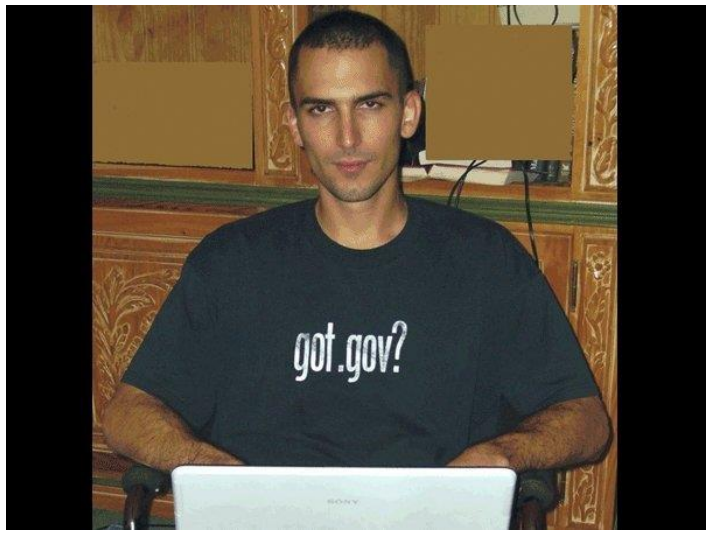
Book : « The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage », Clifford Stoll (1989)

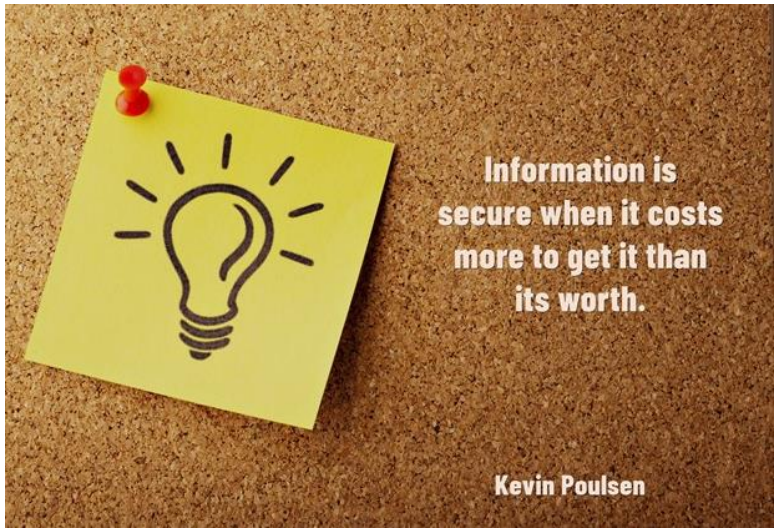
1990's : the rise of Hacktivism and Cybercrime

In the 1990's, more people and corporation were using the Internet. A more ergonomic application Layer, ***the Web (1989)***, give to the network more understandable use case. It technically led to the "2000 Tech bubble".

As notorious cases, Jonathan James ("c0mrade") stole the International Space Station Source Code, the "Electronic Disturbance Theater" hacktivist group launching DDOS against the Pentagon Website or the dark times of now Editor-in-Chief of the Wired Kevin Poulsen ("Dark Dante"). Also countless of world-propagated virus ("I Love You", "Melissa", …)

Also, in 1996 an Interpol working group on ***Transnational Crime*** ("G8 Roma-Lyon Group") acknowledge the threat posed by criminal misusage of new technologies, the opportunity for supporting transnational criminal organization and thus coined the word "cybercrime" to refer broadly about offenses committed with the use of digital technologies.





https://www.nytimes.com/1998/10/31/world/hacktivists-of-all-persuasions-take-their-struggle-to-the-web.html
https://www.coe.int/en/web/cybercrime/the-budapest-convention

2000-2005 : Malicious R&D

In the 2000's, between democratization of high speed DSL lines, USA actions ("War on Terror", Copyright Act, Electronic Child Abuse fighting, …) and progressive adoption of the Tech Bubble innovation, ***cyber attacks expands***.

In February 2000, Michael Calce ("MafiaBoy") DDOSed Yahoo, Amazon, Ebay, Dell, FIFA or CNN ("Project Rivolta"); for personal gains.
Very ***aggressive worms*** popped up regularly ("Anna Kournikova, "SoBig", "Blaster/Sasser"). They generally had an exponential propagation (victims*2 every hour) but were short living (Apogee at H+18).

Between 2001 and 2002, Gary McKinnon ("Solo") scrambled into the US Army and the NASA networks to search for proof of antigravity technologies and alien's contacts. The BBC related to the incident as "*biggest military computer hack of all time*". But in the mean time …

The FBI managed finally in 2004 to remediation to the "Moonlight Maze incident", a sophisticated ***long-standing cyberespionage operation*** that started in 1996 were the Russian Government was blamed. Recent development of the case points toward an ancestor of the *Turla* hacking group, considered by Estonian Foreign Intelligence Service to works for the Russian FSB.

These are also the years were smartphone and mobile internet access developed and the completion of the ***Fixed Mobile Convergence*** (FMC) in most Western countries.

https://en.wikipedia.org/wiki/Moonlight_Maze
https://web.archive.org/web/20070326115414/http://www.fbi.gov/libref/factsfigure/factsfiguresapri2003.htm

1996-2004 : Moonlight Maze

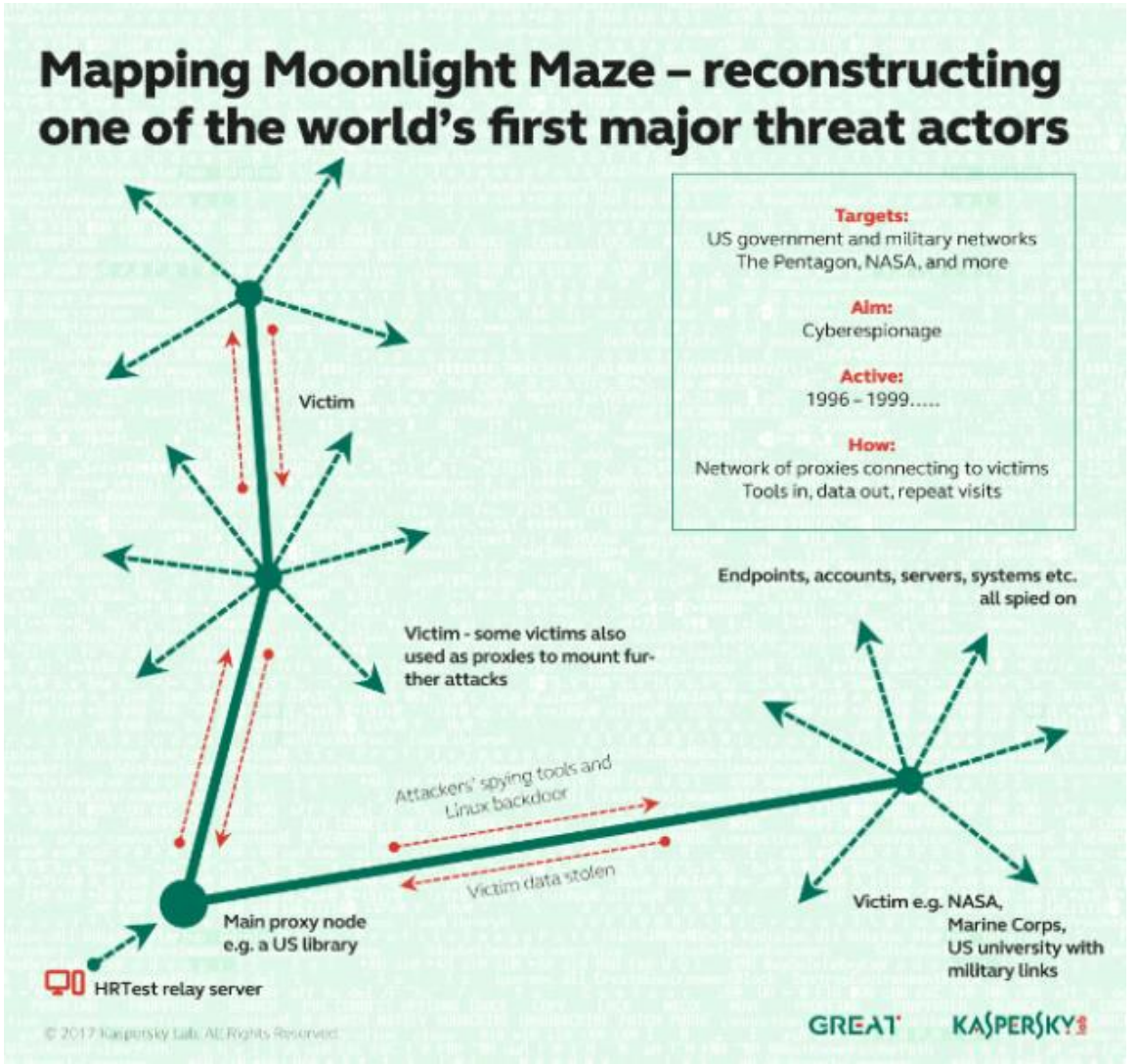
THE SUNDAY TIMES · 25 JULY 1999

OPERATION MOONLIGHT MAZE

Missing secrets

Russian hackers steal US weapons secrets

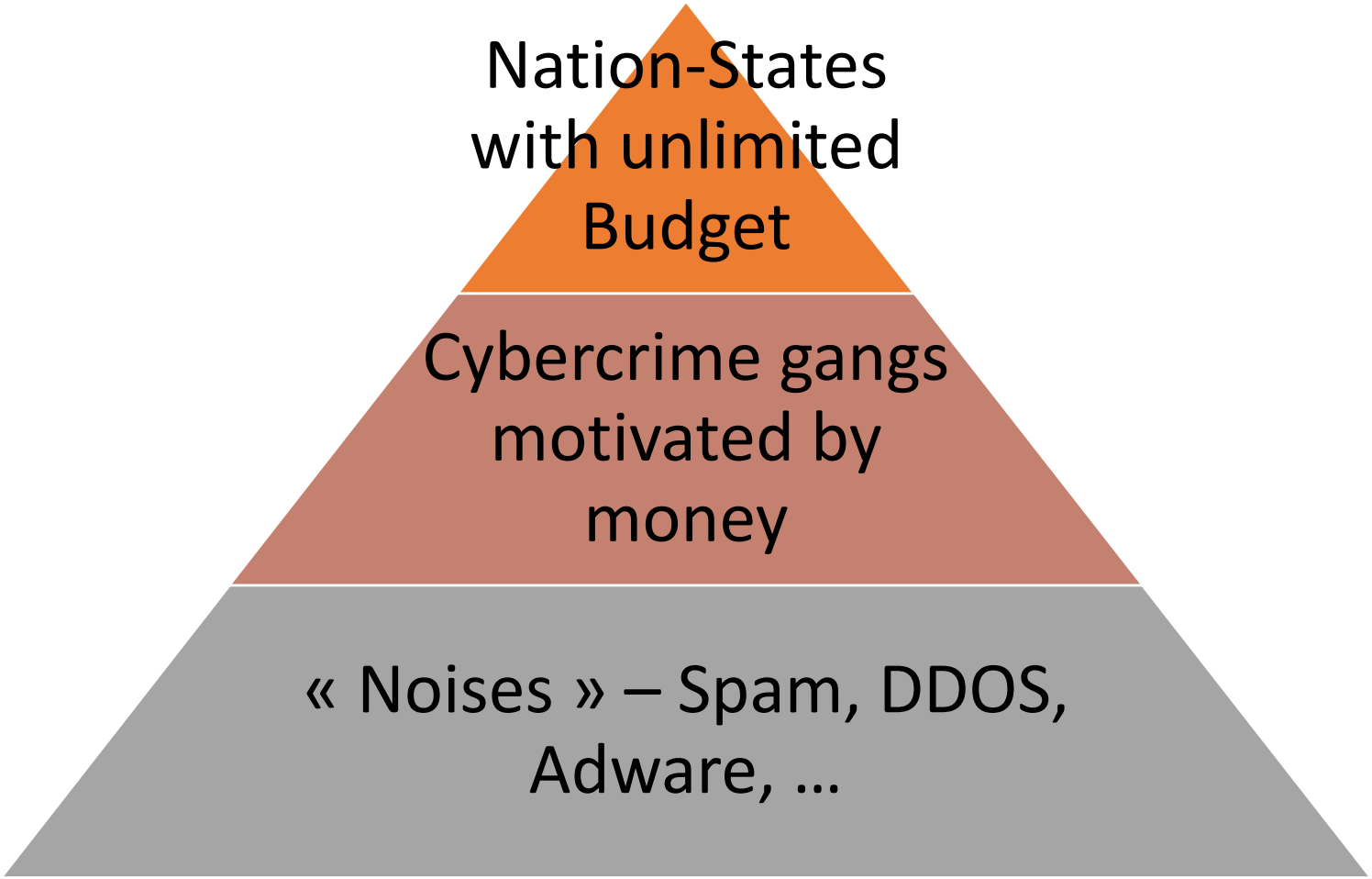
by Matthew Campbell Washington



https://www.newsweek.com/were-middle-cyerwar-166196
https://www.computerworld.com/article/2592630/hunting-hackers--how-to-fight-back.html
https://www.gao.gov/assets/gao-01-341.pdf

2005-2010 : Three separated tracks

The ***offensive activities in Cyberspace*** became more and more scrutinized and DDOS attacks for extorsion exploded. The 2007 DDOS on Estonia as been a shockwave for NATO Countries, and the 2008 Georgian war was a weak signal of the Russian military operation reshaping.



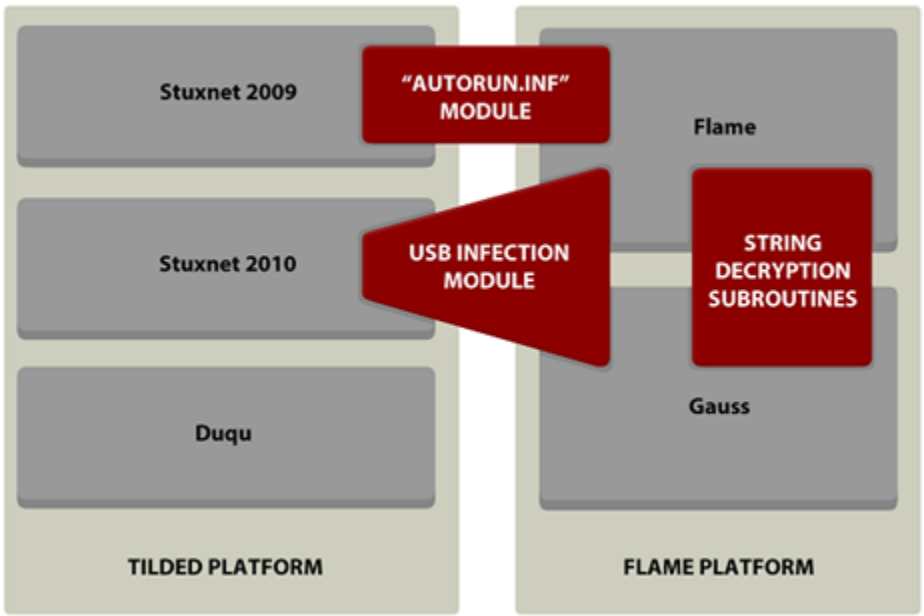
2005-2012 : Stuxnet and « Olympic Games » Operation

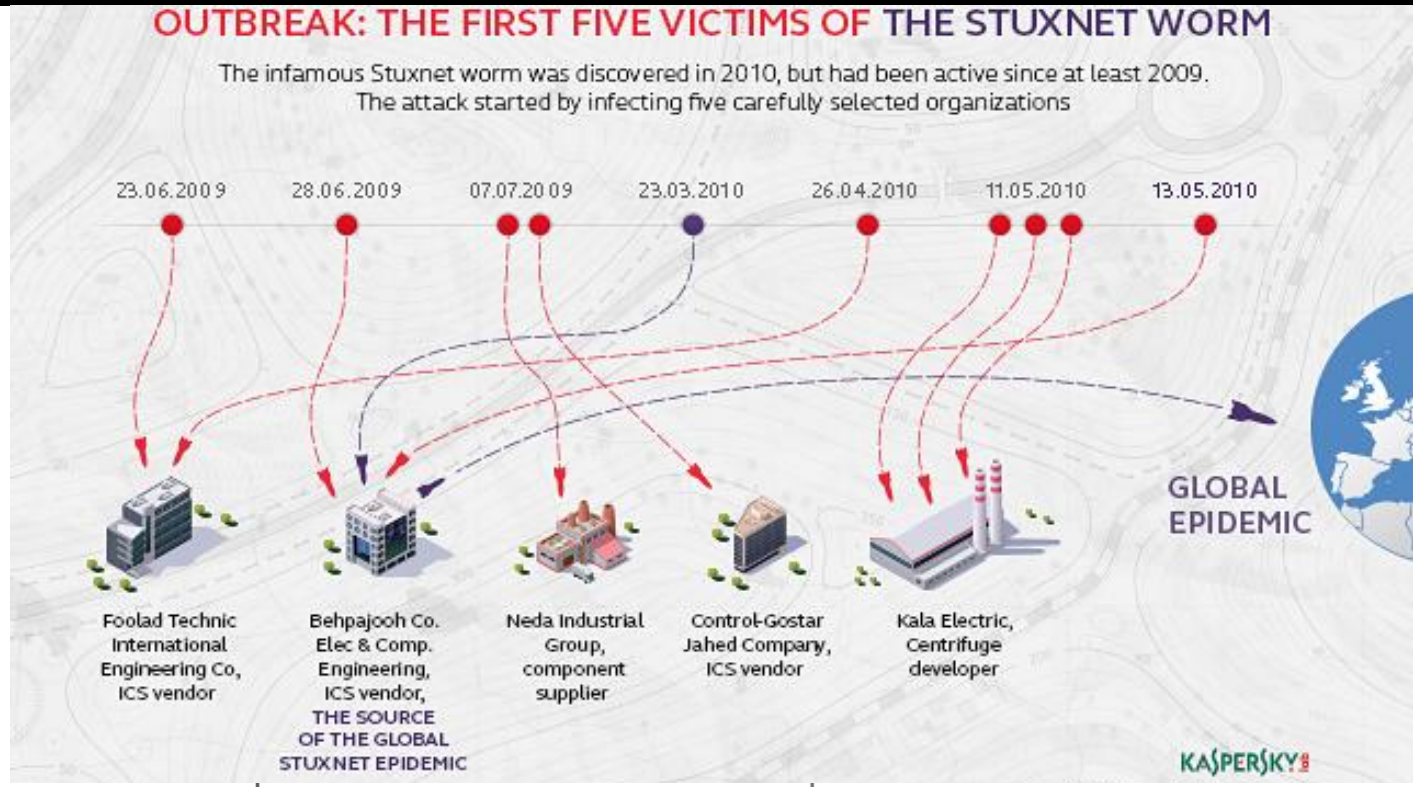
Table 1

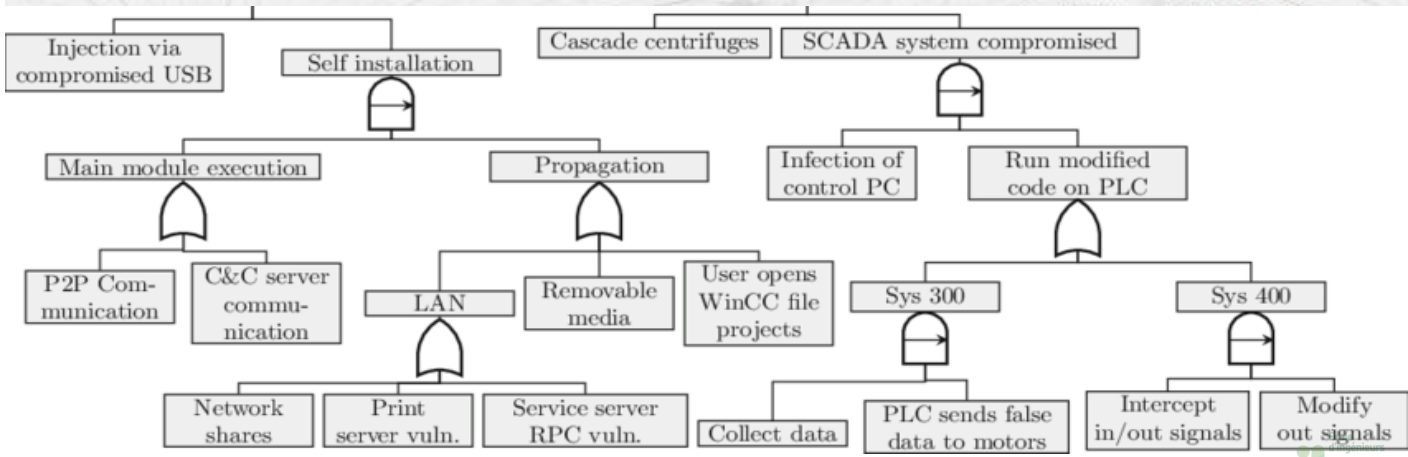
Evolution of Stuxnet versions

Version	Date	Description
0.500	November 3, 2005	C&C server registration
0.500	November 15, 2007	Submit date to a public scanning service
0.500	July 4, 2009	Infection stop date
1.001	June 22, 2009	Main binary compile timestamp
1.100	March 1, 2010	Main binary compile timestamp
1.101	April 14, 2010	Main binary compile timestamp
1.x	June 24, 2012	Infection stop date

The relationship of Stuxnet, Duqu, Flame and Gauss



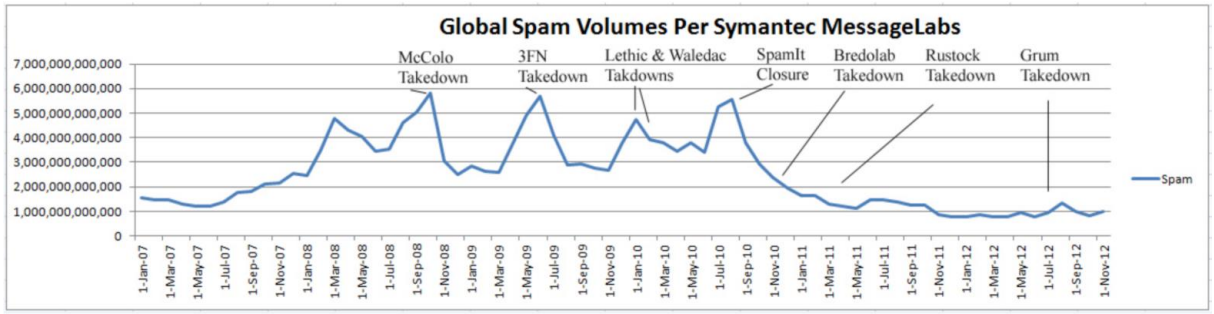


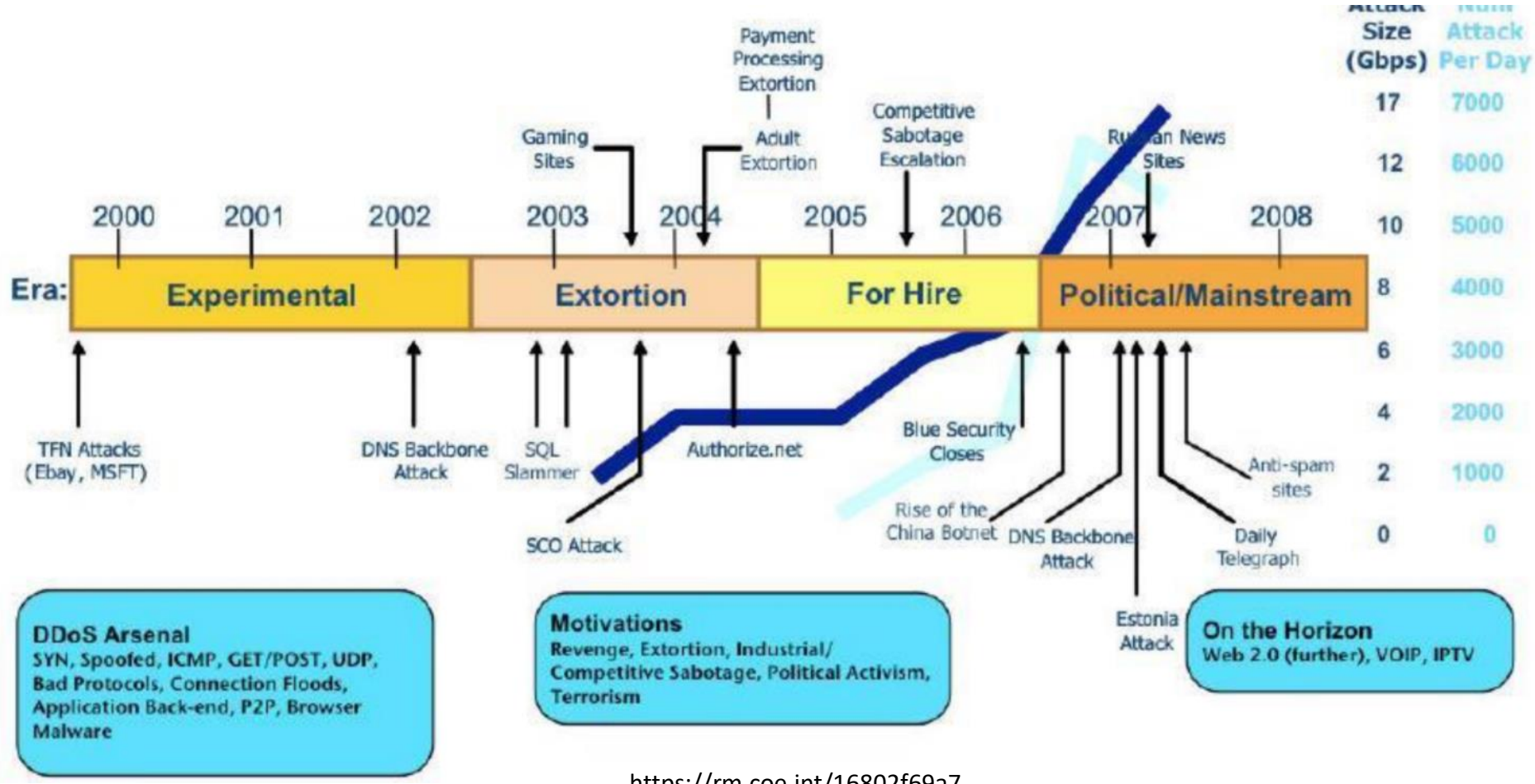


https://docs.broadcom.com/doc/stuxnet-missing-link-13-en

Book : « Countdown to Zero Day », Kim Zetter, 2015

2005-2010 : APT Innovates, Cybercrime industrializes, Hacktivist follows

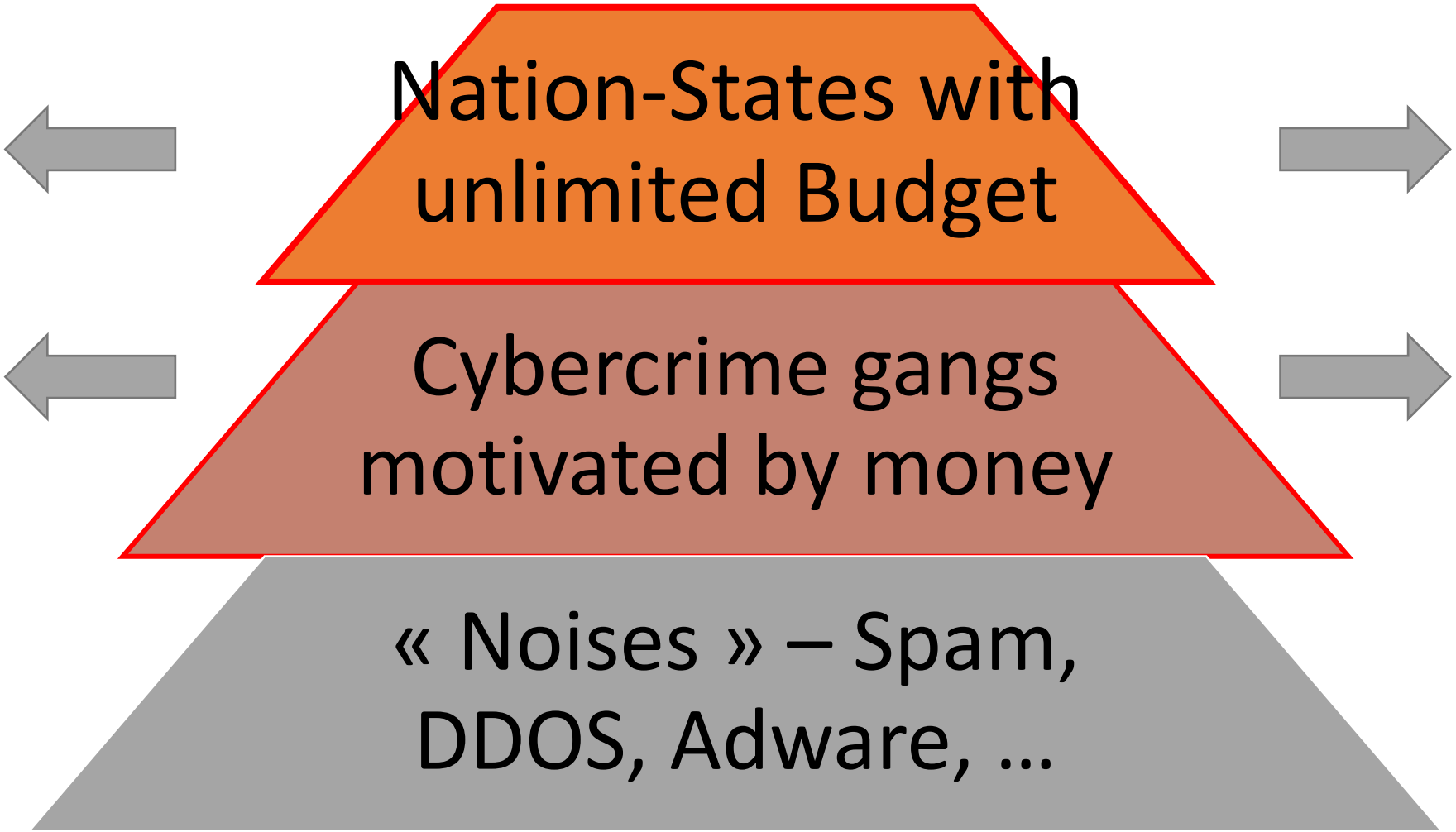




https://rm.coe.int/16802f69a7

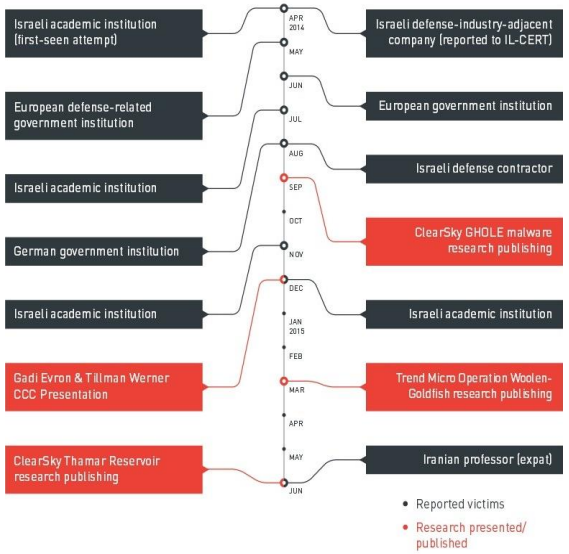
2010-2015 : Big Guys Became Bigger

This period as been very active from a cyber offense point of view. Snowden, ShadowBroker Leaks, Darknet Black Market (DNM), Explosion of ransomware for the general population, North Korea and Iran showing cybermuscle, the USA-China cyberdeal, Russian Doping Scandal counter-attack, not forgetting of course the “Arab Spring” or “Euromaidan” empowered by Social Media.



2010-2015 : Asymetric Warfare Strategies fully integrate Cyber Operations

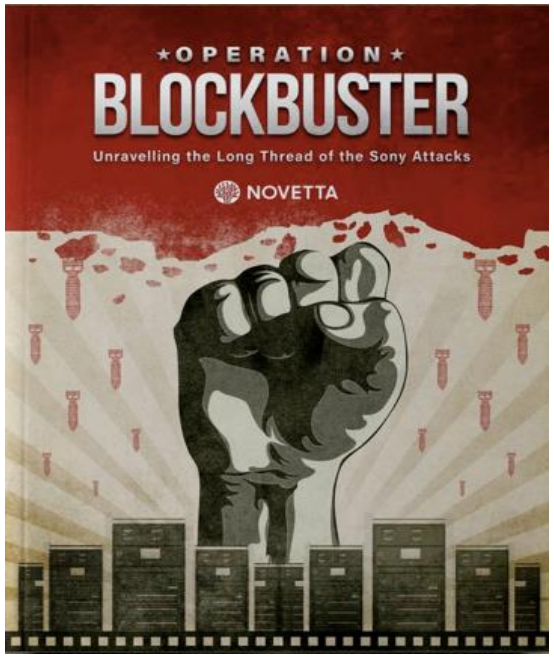
In 2012, Iranian Hacker probably repurpose the « Wiper » malware (linked to OG Flames) to sabotage Saudi Aramco installation. Its successor is refered as « Oilrig » Group.



Timeline of Rocket Kitten-related activities

[Iranian Cyber-Activities]

In 2014, pretexting the movie « The Interview » to be insulting, NK-RGB Bureau 121 (« Lazarus ») launch a cyber attack on Sony Picture International.



https://operationblockbuster.com/

In 2014, following a Crowdstrike report « APT1 », FBI charges for the first time Foreign Military Hacker. This indictment is the first of a long-standing strategy of name and shame.

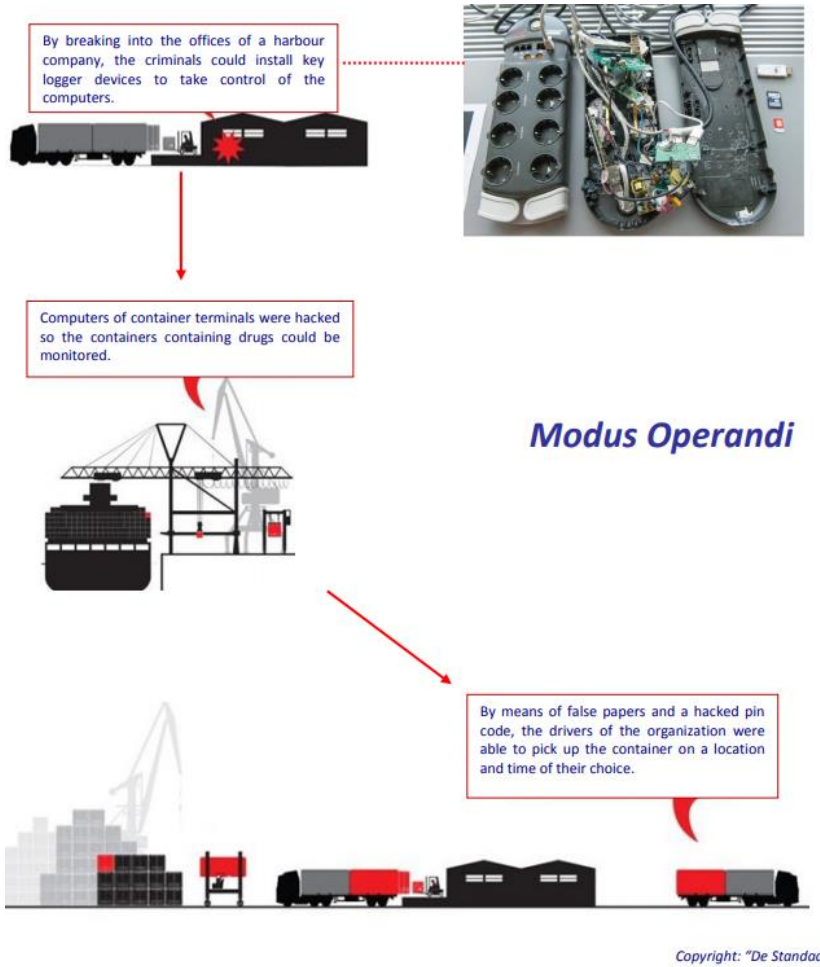
[Us. Charges Five Chinese Military Hackers]

2010-2015 : Organized Crime meets Cyber espionnage

Police warning after drug traffickers' cyber-attack

By Tom Bateman
Reporter, Today programme

16 October 2013



https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/
https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf

FBI uncovers cyber insider trading gang

Nine suspects are expected to be charged in the US with insider trading based on corporate press releases stolen by hackers before they had been made public

By **Warwick Ashford,** Senior analyst

Published: **11 Aug 2015 13:30**

US authorities have arrested nine suspected insider traders who relied on hackers to steal commercially sensitive corporate information from newswire services.

The suspects are expected to be charged on 11 August 2015 in Brooklyn, New York and New Jersey in connection with insider trading based on stolen corporate press releases before they had been made public, reports *Bloomberg News*.

The hackers – believed to be based in Ukraine and possibly Russia – broke into the computer systems of PRNewswire Association, Marketwired and Business Wire.

Information stolen by the hackers is believed to have been used by their associates in the US to buy and sell shares of dozens of companies, including Boeing, Hewlett-Packard and Oracle, to make more than $30m in profit.

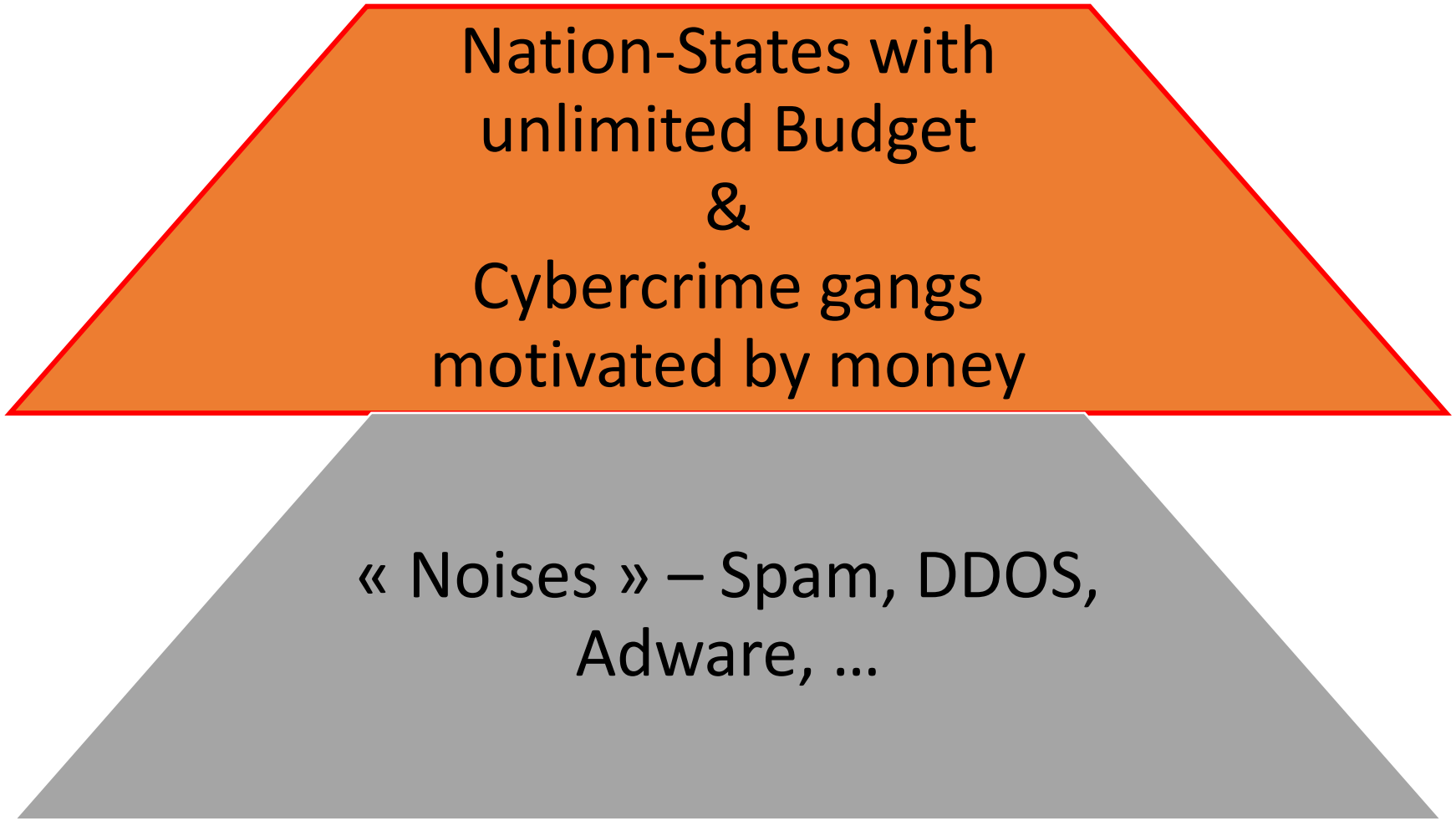
The case reportedly marks the first time prosecutors have alleged that a securities fraud scheme was based on hacked inside information and it is also the largest known suspected case of hacking that resulted in insider trading.

https://www.computerweekly.com/news/4500251471/FBI-uncovers-cyber-insider-trading-gang
https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/nine-people-charged-in-largest-known-computer-hacking-and-securities-fraud-scheme

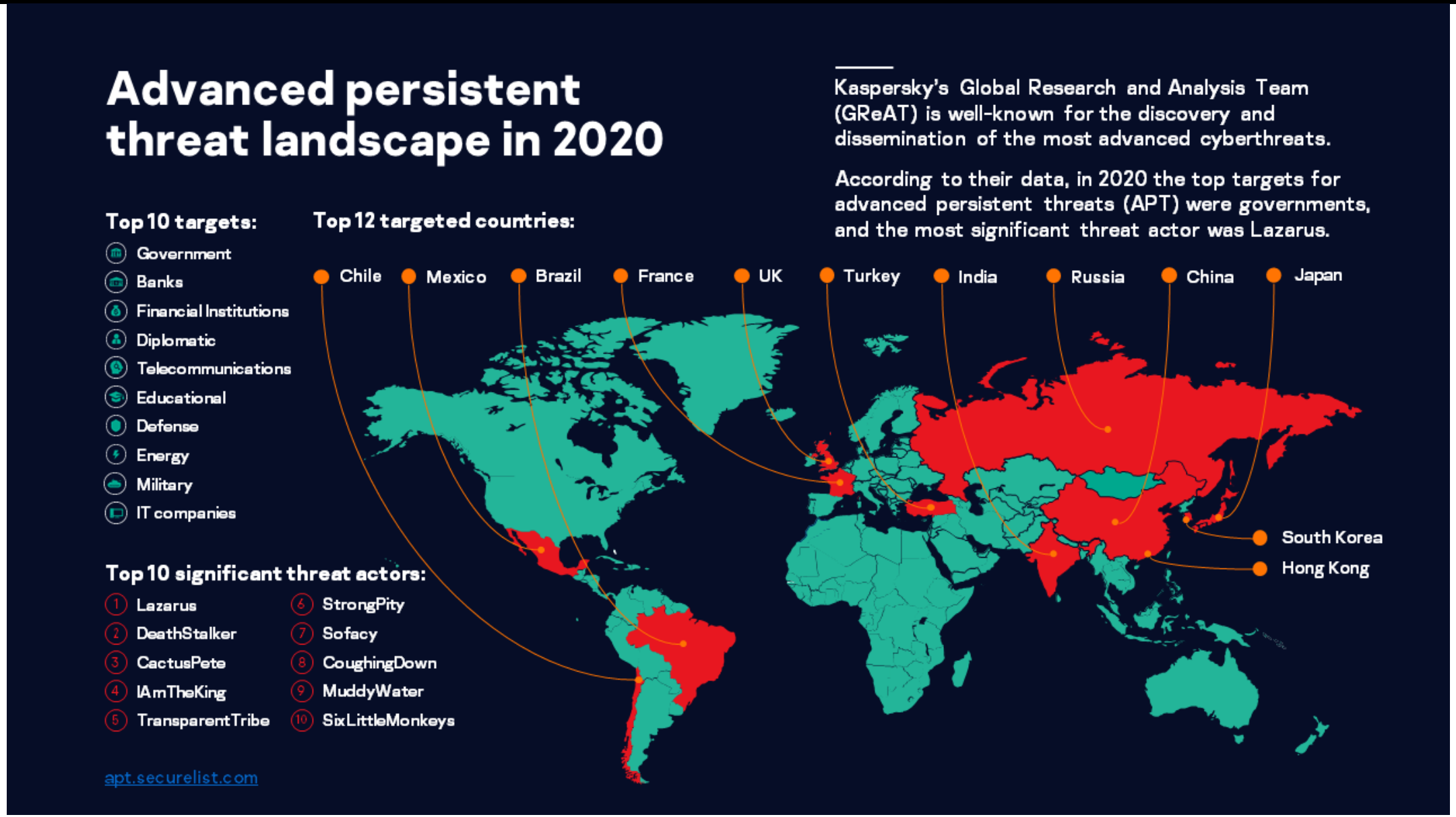
Conclusion

2015-2021 : Is that a Mouse or a Elefant ?

Increasing availability of open sources or leaked offensive tools, as well as materials covering advanced modus operandi, weaponized by adversaries of all degree of sophistication blurred the lines of Threat Analysis. Less custom malware, more False-Flags, more Cybercrime Gangs using APT's techniques, more APTs using cybercrime for fundings.



APTs ecosystems



https://securelist.com/apt-predictions-for-2021/99387/

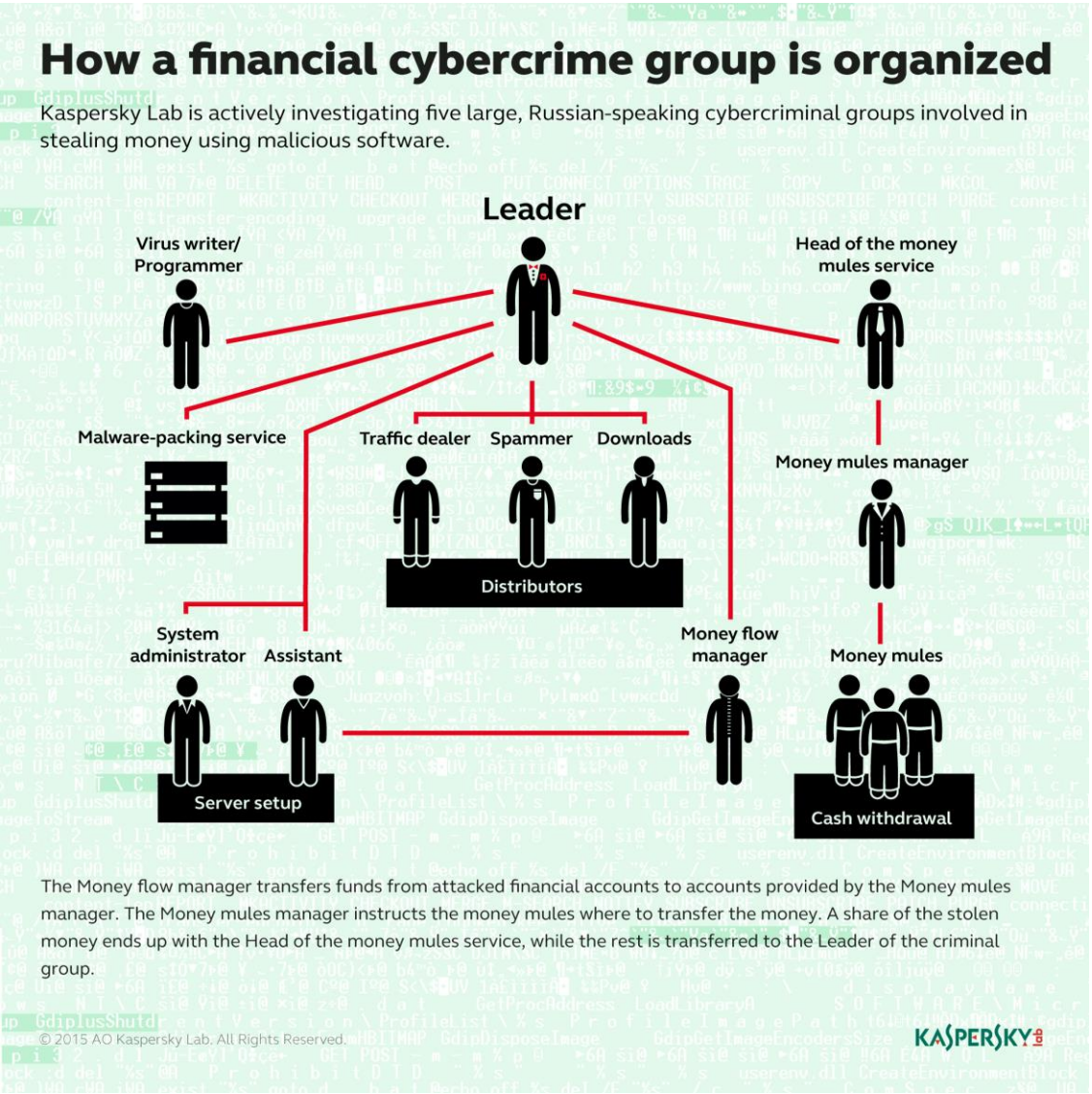
APTs ecosystems

TABLE 12: Matching characteristics between APT1 and Unit 61398

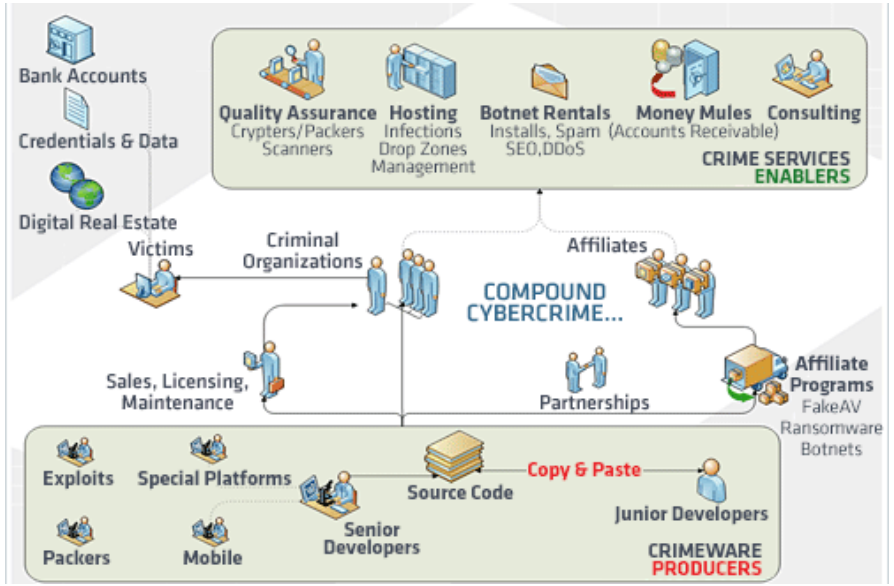
Characteristic	APT1 (as directly observed)	Unit 61398 (as reported)
Mission area	» Steals intellectual property from English-speaking organizations » Targets strategic emerging industries identified in China's 12th Five Year Plan	» Conducts computer network operations against English-speaking targets
Tools, Tactics, and Procedures (TTPs)	» Organized, funded, disciplined operators with specific targeting objectives and a code of ethics (e.g., we have not witnessed APT1 destroy property or steal money which contrasts most "hackers" and even the most sophisticated organize crime syndicates)	» Conducts military-grade computer network operations
Scale of operations	» Continuously stealing hundreds of terabytes from 141 organizations since at least 2006; simultaneously targeting victims across at least 20 major industries » Size of "hop" infrastructure and continuous malware updates suggest at least dozens (but probably hundreds) of operators with hundreds of support personnel	» As part of the PLA, has the resources (people, money, influence) necessary to orchestrate operation at APT1's scale » Has hundreds, perhaps thousands of people, as suggested by the size for their facilities and position within the PLA
Expertise of personnel	» English language proficiency » Malware authoring » Computer hacking » Ability to identify data worth stealing in 20 industries	» English language requirements » Operating system internals, digital signal processing, steganography » Recruiting from Chinese technology universities
Location	» APT1 actor used a Shanghai phone number to register email accounts » Two of four "home" Shanghai net blocks are assigned to the Pudong New Area » Systems used by APT1 intruders have Simplified Chinese language settings » An APT1 persona's self-identified location is the Pudong New Area	» Headquarters and other facilities spread throughout the Pudong New Area of Shanghai, China
Infrastructure	» Ready access to four main net blocks in Shanghai, hosted by China Unicom (one of two Tier 1 ISPs in China) » Some use of China Telecom IP addresses (the other Tier 1 ISP)	» Co-building network infrastructure with China Telecom in the name of national defense

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

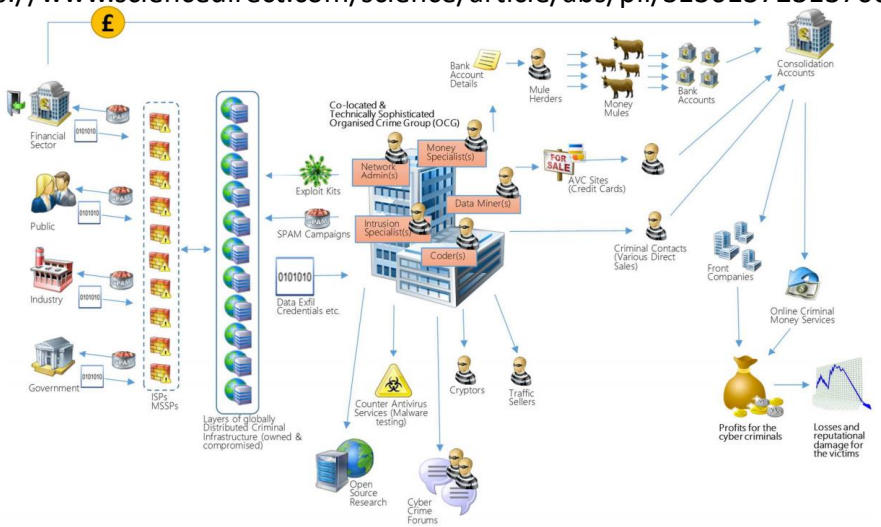
Cybercrime ecosystems



https://securelist.com/russian-financial-cybercrime-how-it-works/72782/

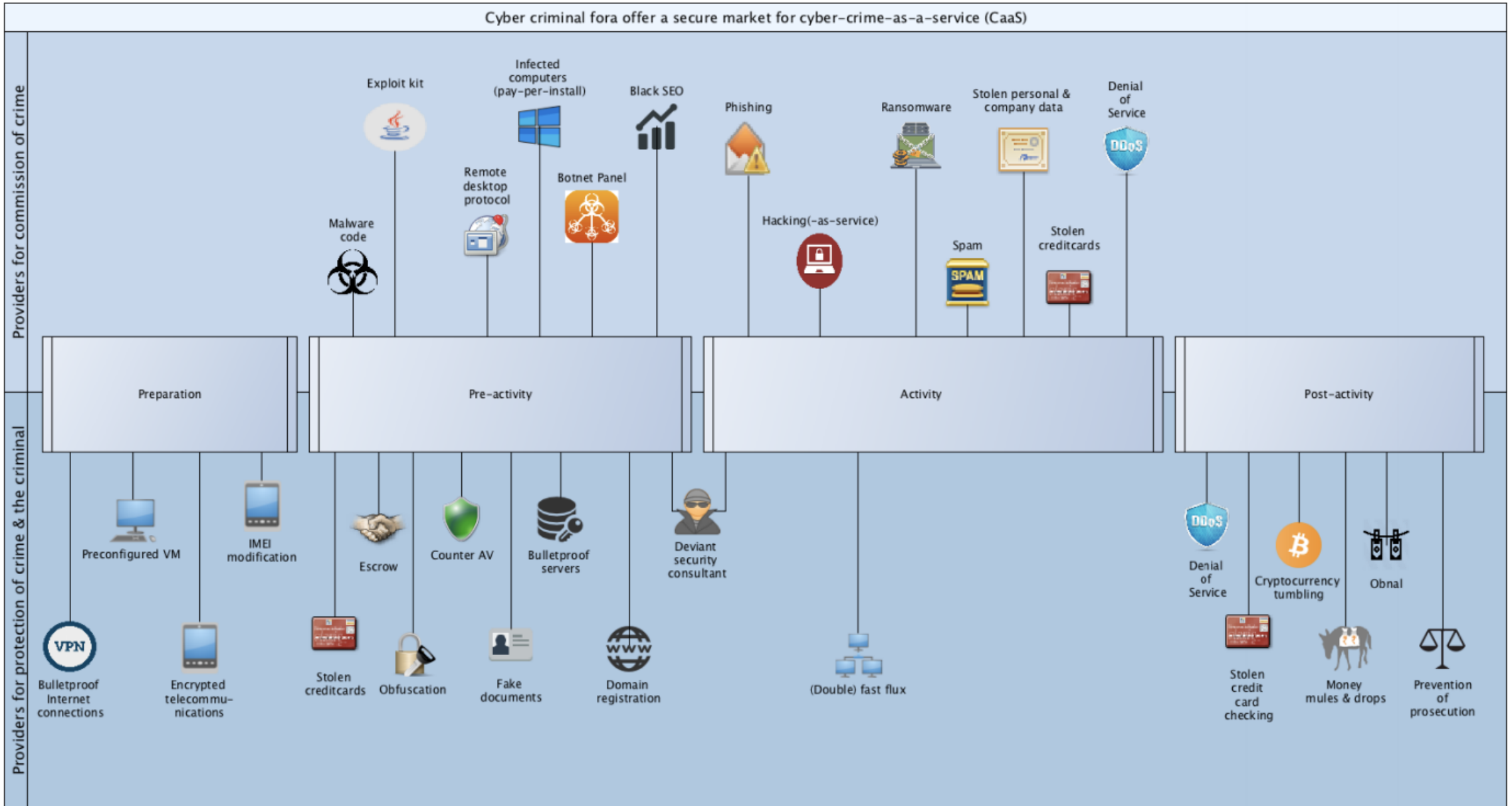


https://www.sciencedirect.com/science/article/abs/pii/S1361372313700538



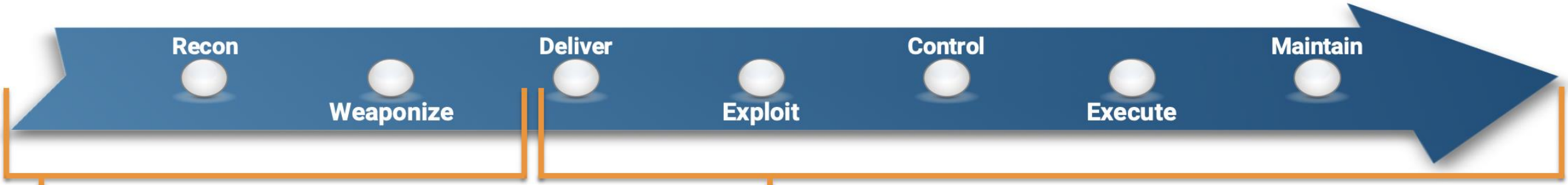
https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity

Cybercrime ecosystems



https://researchinformation.bris.ac.uk/ws/portalfiles/portal/194364696/DEVIANT_SECURITY_EHAVANDESANDT.pdf

The Magnitude of the « Kill Chain »



PRE-ATT&CK

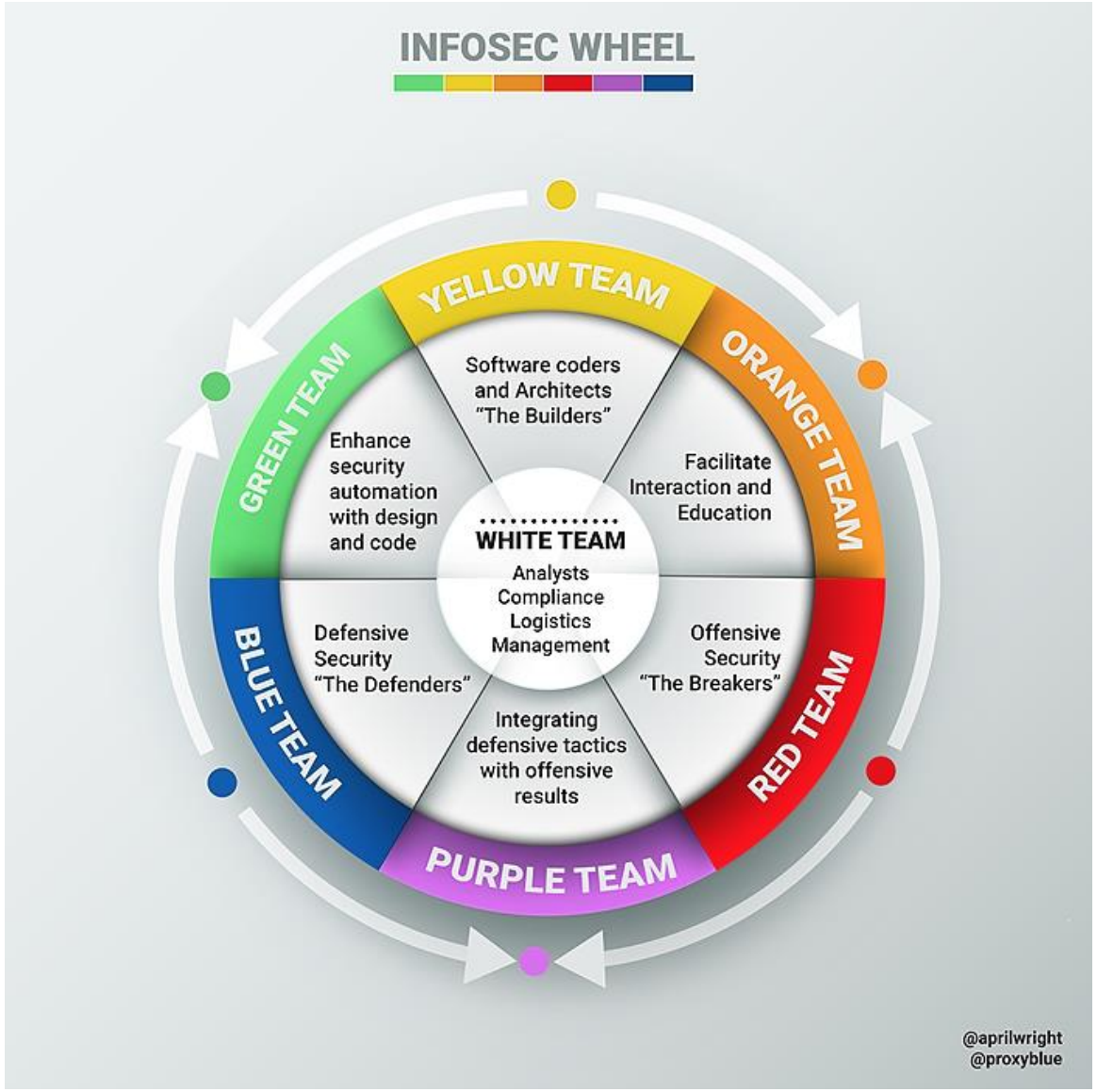
- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Weakness Identification
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

https://attack.mitre.org/resources/enterprise-introduction/

The Magnitude of the « Infosec Wheel»



https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700


École
d'ingénieurs
ensibs :
Université Bretagne Sud