CYBERCOERCITION

LA NOUVELLE CYBERGUERRE MONDIALE

Bernard BARBIER

@barbier_bernard

linkedin.com/in/bernard-barbier-52538459

bernard.barbier@bbcyber.fr

Ingénieur de l'École Centrale de Paris 1976,

Master en Physique des Plasmas

Membre de l'académie des technologies

Président de BBCyber SAS

-2014-2018 : CAPGEMINI, responsable de la cybersécurité du groupe, responsable de la cyberdéfense interne pour toutes les entités CAPGEMINI dans le monde. 55 pays, 210 000 personnes

-2006-2013 : Directeur technique à la DGSE (équivalent du directeur de la NSA aux États-Unis), en charge du renseignement technique français : SIGINT, IMINT, Cyber Int, cyber opération et cyberdéfense

-2003-2006 : Directeur du LETI (Minatec Grenoble), l'un des meilleurs laboratoires de recherche au monde, dans le domaine de la nanoélectronique et des nanotechnologies (1500 chercheurs)

-2000-2003 : Directeur des Systèmes d'information du Commissariat à l'Energie Atomique (CEA)

La CYBERCOERCITION: un nouveau défi stratégique

OPINIONS • CYBERESPIONNAGE

Cybercoercition : un nouveau défi stratégique

TRIBUNE

Collectif

Face aux cyberattaques, la France doit se doter d'une capacité de dissuasion autonome, écrivent Bernard Barbier, (ex-DT de la DGSE), Edouard Guillaud (ex-CEMA) et Jean-Louis Gergorin (ex-Quai d'Orsay).

Publié le 28 janvier 2020 à 01h38 - Mis à jour le 28 janvier 2020 à 09h44 | Lecture 4 min.

Article réservé aux abonnés

Tribune. Alors que des doutes planent sur la pérennité de la solidarité transatlantique et sur la capacité de l'Europe à s'y substituer, la France doit réagir à deux défis majeurs pour ses intérêts vitaux.

CYBERCOERCITION et DISSUASION nucléaire: deux moyens complémentaires

La coercition est l'action de contraindre quelqu'un, pour le forcer à agir ou à s'en abstenir. Elle existe notamment par contrainte physique ou psychologique. En droit pénal, on parle d'un délit de contrainte.

La Cybercoercition c'est l'action de contraindre, par des attaques cyber répétées, le ou les dirigeants d'un pays, à s'abstenir d'agir et plutôt de réagir.
C'est une arme d'emploi

La dissuasion nucléaire se fonde sur la peur, dans les deux camps, du recours par l'autre à l'arme **nucléaire**. La **dissuasion** consiste à prévenir un acte en persuadant l'acteur concerné que les coûts d'une telle action excèdent ses bénéfices.
C'est une arme de non emploi

Un futur CYBER PEARL HARBOR ?

Cyberattaques : "une grande crise est possible et comporte un risque systémique" (Guillaume Poupard, ANSSI)

ENTRETIEN EXCLUSIF. La prochaine grande crise mondiale sera-t-elle cybercriminelle ? C'est un risque de plus en plus sérieux que n'écartent pas les Etats, y compris la France. Guillaume Poupard, le directeur de l'Agence nationale de la sécurité des systèmes d'information (Anssi), est pourtant optimiste : si toutes les entreprises et les organisations "prennent conscience que tout le monde est attaqué" et investissent dans leur cybersécurité en considérant qu'il s'agit désormais d'une "dépense vitale", alors il est possible de "stopper dans les cinq prochaines années l'explosion actuelle des cyberattaques", qui ont déjà augmenté de 60% en 2021 après avoir quadruplé en 2020. Pierre angulaire de la révolution numérique, la cybersécurité est aussi l'une des clés de la souveraineté technologique européenne. Guillaume Poupard appelle la France à ne pas oublier les acteurs européens du cloud au profit des Gafam américains, et à profiter de la présidence française de l'UE, au premier semestre 2022, pour définir "l'Europe de la cyber", étendre la portée de la directive NIS et créer des "pompiers cyber européens" capables d'intervenir partout.

Un futur CYBER PEARL HARBOR ?

Des Menaces venant des états

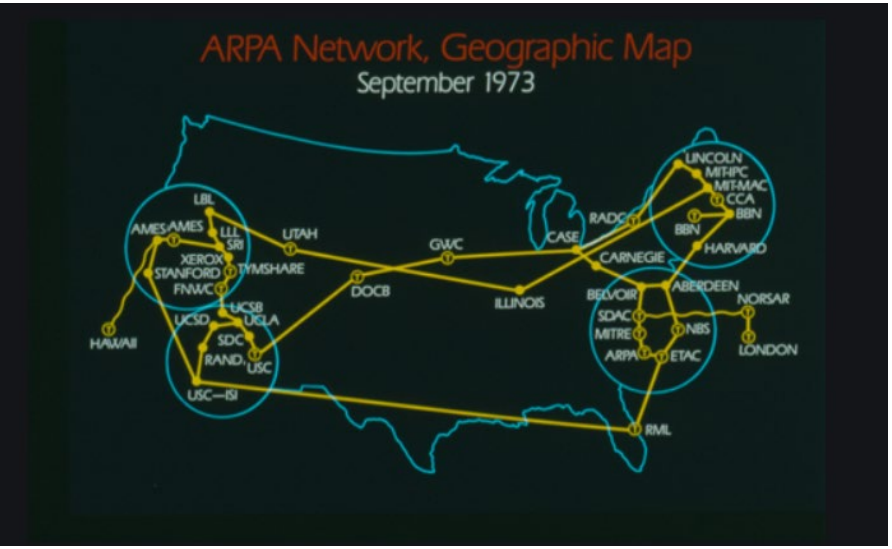
Cyberdéfense de l'ANSSI à Paris (JC/RF)

Des actes de cyberguerre

Pour le directeur général Guillaume Poupard, les attaques les plus inquiétantes sont « *celles où l'attaquant prend pied dans les réseaux et se propage de manière extrêmement discrète mais on ne sait pas ce qu'il veut faire. L'hypothèse la plus probable est qu'il s'agit de services étatiques qui préparent des conflits numériques de demain.* ». Selon Guillaume Poupard, « *si chaque service offensif commence à se pré-positionner chez tout le monde, le risque est grand de construire un baril de poudre auquel il ne manquera plus qu'une étincelle* ».

UN PEU D'HISTOIRE

La création d'INTERNET (ARPANET)



1969 Les deux premiers nœuds D'ARPANET sont reliés.

Le premier message d'ordinateur à ordinateur part d'une machine de l'équipe de KLEINROCK à UCLA (Université de Californie à Los Angeles) pour une machine de l'équipe d'ENGELBART à la Stanford Research Institute (SRI).

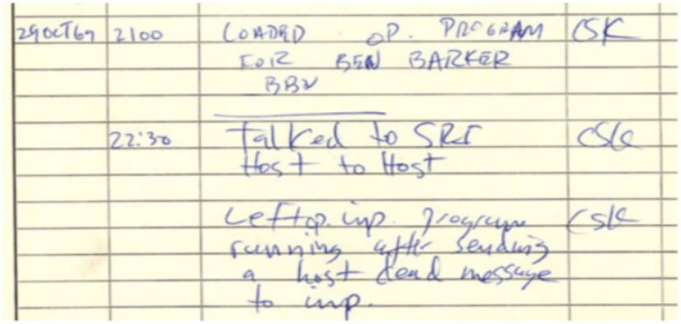
1972 Network Control Protocole (NCP)

Début de la réflexion sur le TCP/IP (KAHN, CERF, 1973)

1978 Le TCP/IP est achevé

1983 Transition d'ARPANET au protocole TCP/IP

Séparation MILNET / ARPANET

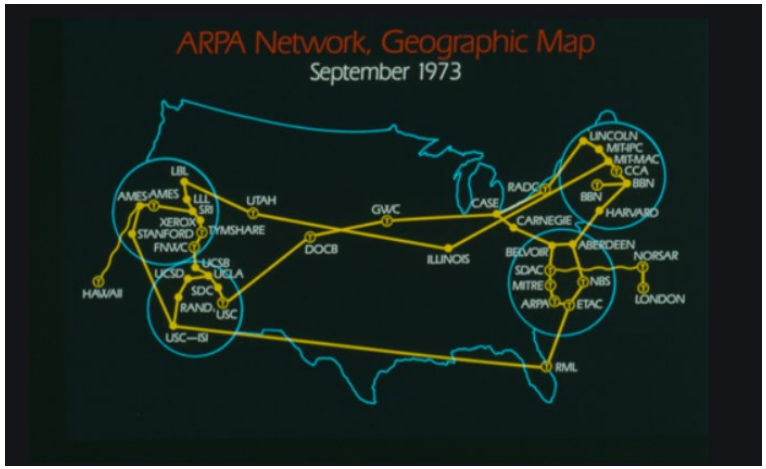


Historical document: First ARPANET IMP log: the first message ever sent via the ARPANET, 10:30 pm, 29 October 1969. This IMP Log excerpt, kept at UCLA, describes setting up a message transmission from the UCLA SDS Sigma 7 Host computer to the SRI SDS 940 Host computer

UN PEU D'HISTOIRE
WARGAMES

1983, WAR GAMES, film qui montre un lycéen qui pirate par hasard le système du NORAD,

1983, USA, suite au film WARGAMES, le président REAGAN: *could something like this really happen* réponse du CEMA, *Mr President, the problem is much more worse than you think*..



•Les cyber attaques majeures

STUXNET 2010

•Les cyber attaques majeures

UKRAINE 2016

New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction

A fresh look at the 2016 blackout in Ukraine suggests that the cyberattack behind it was intended to cause far more damage.

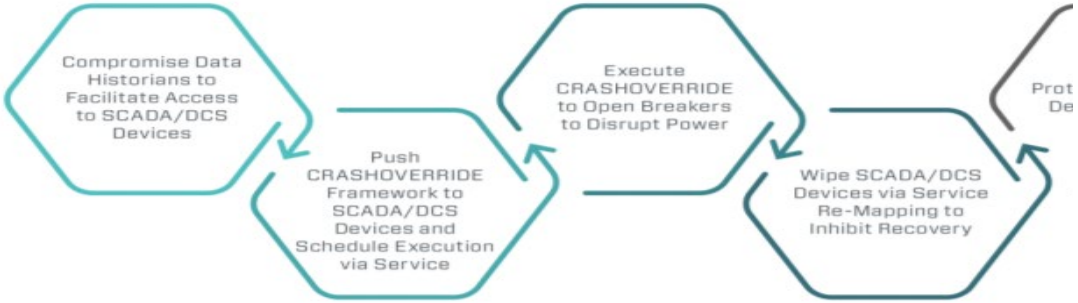
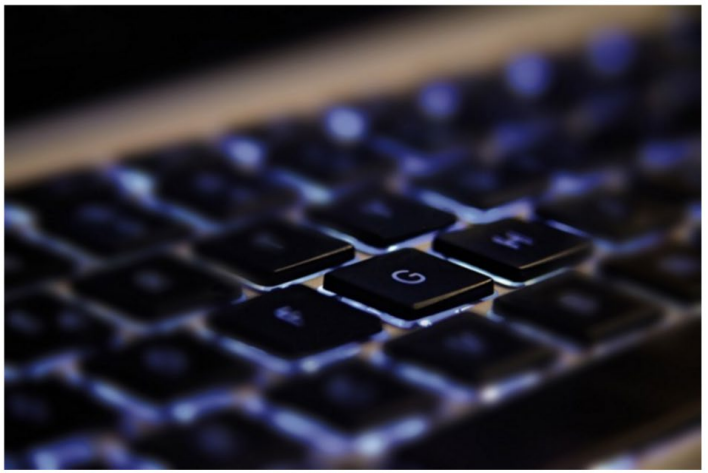


Figure 1: CRASHOVERRIDE Event Attack Flow

Ukraine : 700 000 personnes dans le noir après une cyber-attaque

FABRICE DEPREZ
26 Janvier 2016

Fin décembre, une cyber-attaque a entraîné une panne d'électricité géante dans l'ouest de l'Ukraine. Les circonstances sont encore floues, mais les regards se tournent déjà vers la Russie.



Crédit Pixies / Pixabay

La coupure n'aura duré que quelques heures et serait sans doute restée dans l'ombre de l'actualité internationale si, le lendemain, la nouvelle n'était pas tombée : un sabotage serait responsable de la panne qui a plongé dans le noir 700 000 personnes de la région d'Ivano-Frankivsk, dans l'ouest de l'Ukraine, en fin d'année 2015.

•Les cyber attaques majeures

WANACRY 12 MAI 2017

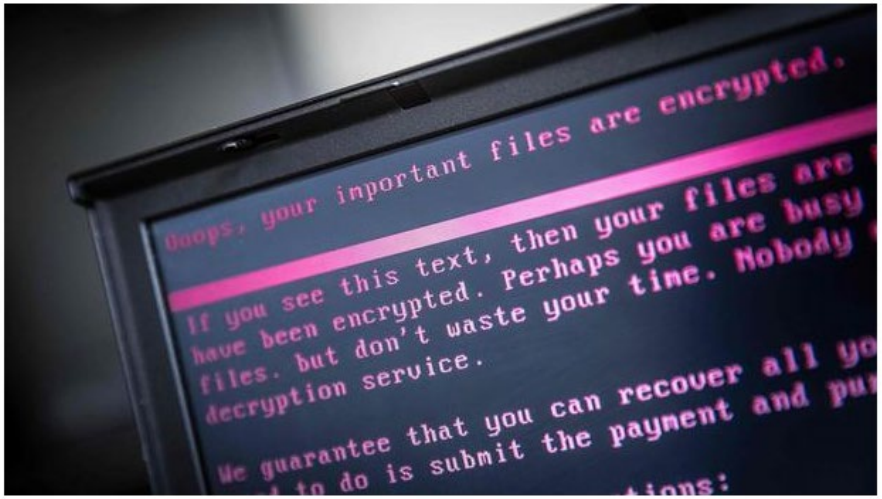
•Les cyber attaques majeures

NOT PETYA 27 Juin 2017

Cyberattaque Petya : le but du virus serait de détruire les fichiers

VIDÉO - L'attaque informatique qui s'est propagée hier a perturbé les systèmes de grandes entreprises et d'administrations. Le secrétaire d'État chargé du Numérique évoque un niveau d'attaque «sans précédent».

Par **Benjamin Ferran**
Publié le 28 juin 2017 à 10:42, mis à jour le 29 juin 2017 à 11:22



•Les cyber attaques majeures

les rançonslogiciels: 2019

Global ransomware damage costs. PHOTO: Cybercrime Magazine.

Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021

Le ransomware Clop serait à l'origine de la cyberattaque du CHU de Rouen : les détails de l'ANSSI

Alexandre Boero Contributeur
28 novembre 2019 à 13h43

26

© Pixabay

Clop, le rançongiciel, a été identifié par les services français au début de l'année. Il est principalement distribué sous forme d'une campagne d'hameçonnage, comme ce fut visiblement le cas pour le centre hospitalier normand.

Ransomware is expected to attack a business every 11 seconds by the end of 2021

SUNBURST-SOLARWINDS, UNE SURPRISE STRATEGIQUE,

•Les cyber attaques majeures

KASEYA, REVIL: 2 juillet 2021

Un message sur une porte close d'un magasin Coop en Suède indiquant qu'un "problème informatique" empêche l'ouverture de l'enseigne. AP - Jonas Ekstromer

"Nous avons compromis plus d'un million d'ordinateurs. Si quelqu'un veut négocier l'obtention d'un outil de décryptage universel, notre prix est de 70 millions de dollars, payables en bitcoin", ont annoncé les pirates informatiques, dans un message posté sur le blog de REvil, le groupe de cybercriminels russes soupçonné d'être à l'origine de l'opération.

BBCyber

Les cyber attaques majeures
Espionnage massif des chinois
19 juillet 2021

U.S. Accuses China of Hacking Microsoft

The Biden administration organized a broad group of allies to condemn Beijing for cyberattacks around the world, but stopped short of taking concrete punitive steps.

403

The Biden administration announced it would join a group of NATO allies to condemn China for cyberattacks, which in the past have caused harm to United States businesses and organizations. Sarahbeth Maney/The New York Times

•Les cyber attaques majeures

Colonial Pipeline

L'oléoduc Colonial toujours bloqué, Biden tire les leçons de la cyber attaque

Après l'attaque informatique qui a imposé l'arrêt du principal oléoduc de la côte Est des Etats-Unis, Colonial Pipeline prévoit une remise en service progressive d'ici à la fin de la semaine. La Maison-Blanche veut renforcer les lignes de défense des entreprises privées.

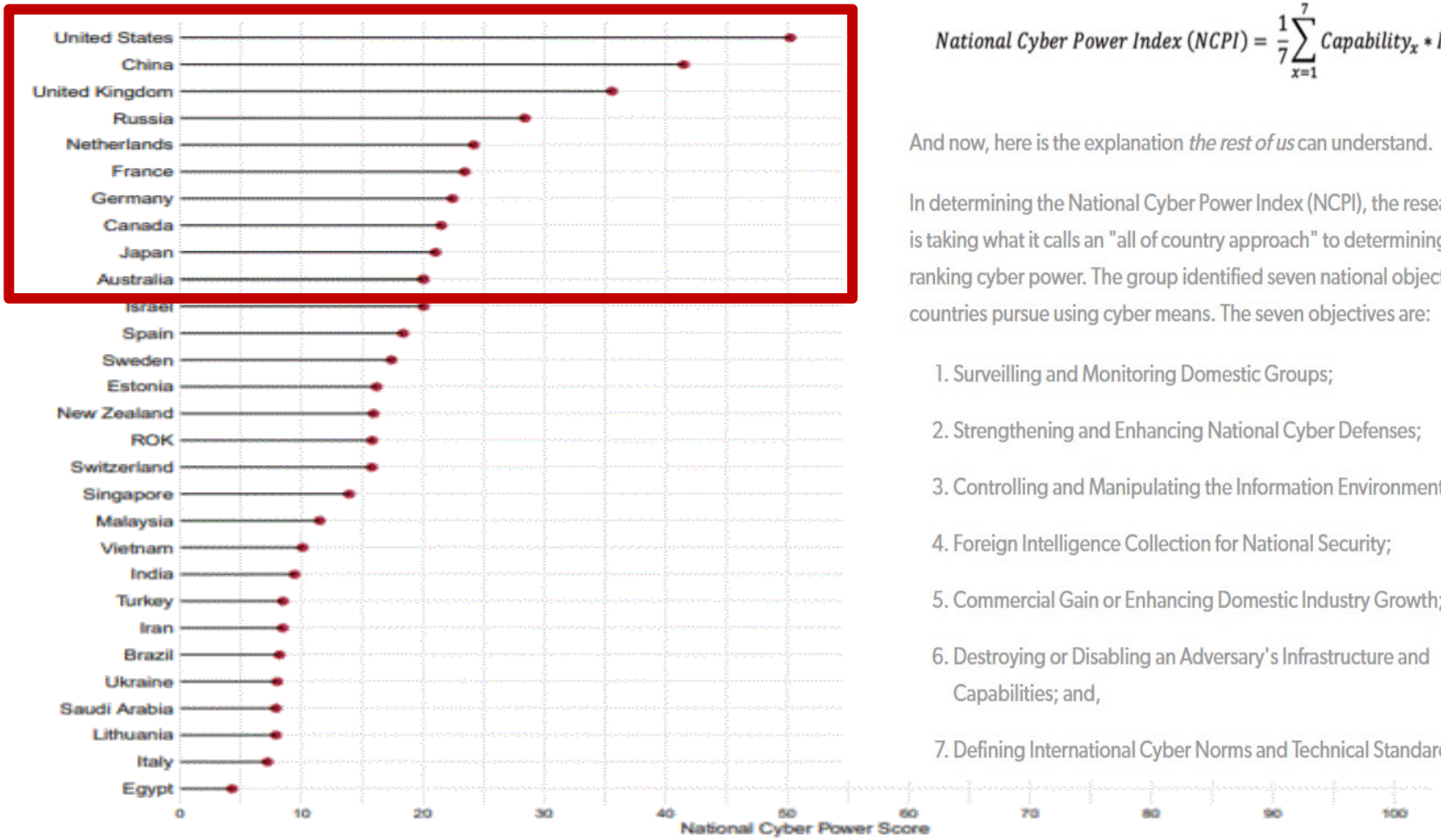
Lire plus tard | Énergie & Environnement | Partager | Commenter

Colonial Pipeline transporte en temps normal 45 % de la consommation de produits raffinés de la côte Est. (Kevin G. Hall/TNS/ZUMAPRESS. com/Réa)

Par **Véronique Le Billon**

LES CYBER PUISSANCES

Graph 1: NCPI 2020: Most Comprehensive Cyber Powers



$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

And now, here is the explanation *the rest of us* can understand.

In determining the National Cyber Power Index (NCPI), the research team is taking what it calls an "all of country approach" to determining and ranking cyber power. The group identified seven national objectives that countries pursue using cyber means. The seven objectives are:

1. Surveilling and Monitoring Domestic Groups;
2. Strengthening and Enhancing National Cyber Defenses;
3. Controlling and Manipulating the Information Environment;
4. Foreign Intelligence Collection for National Security;
5. Commercial Gain or Enhancing Domestic Industry Growth;
6. Destroying or Disabling an Adversary's Infrastructure and Capabilities; and,
7. Defining International Cyber Norms and Technical Standards.

LES CYBER PUISSANCES DU MAL

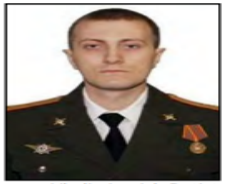
Les Cyber espions Russes

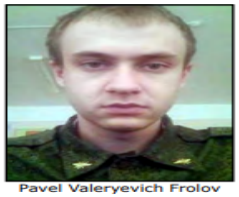
WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft


Yuriy Sergeyevich Andrienko


Sergey Vladimirovich Detistov


Pavel Valeryevich Frolov


Anatoliy Sergeyevich Kovalev


Artem Valeryevich Ochichenko


Petr Nikolayevich Pliskin

REMARKS

On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officers for their alleged roles in targeting and compromising computer systems worldwide, including those relating to critical infrastructure in Ukraine, a political campaign in France, and the country of Georgia; international victims of the "NotPetya" malware attacks (including critical infrastructure providers); and international victims associated with the 2018 Winter Olympic Games and investigations of nerve agent attacks that have been publicly attributed to the Russian government. The indictment charges the defendants, Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin, with a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victims' computers. The indictment also charges these defendants with false registration of a domain name, conspiracy to commit wire fraud, wire fraud, intentional damage to protected computers, aggravated identity theft, and aiding and abetting those crimes. The United States District Court for the Western District of Pennsylvania issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

LES CYBER PUISSANCES DU MAL

Les Cyber Corsaires Russes

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich

Alleged Russian Hacker Behind $100 Million Evil Corp Indicted

The US is charging Maksim Yakubets over two of the biggest cybertheft campaigns of the last decade, and offers a record reward for information on t case.

Le plus grand cyber-escroc du monde démasqué en tant qu'ancien agent de renseignement russe

Maksim Yakubets, 32 ans, a été nommé le plus grand cybercriminel du monde après avoir dirigé le groupe de cybercriminalité le plus dangereux du monde, Evil Corp

Un pirate informatique russe accusé de tromper des victimes britanniques sur des centaines de millions de livres a été désigné comme le plus grand cybercriminel du monde.

Maksim Yakubets, 32 ans, a éclaboussé un tigre de compagnie et des lionceaux, et possède une Lamborghini personnalisée avec une plaque d'immatriculation qui lit THIEF en russe.

Il est décrit comme intouchable à Moscou, où il se filme régulièrement au volant de «beignets» autour de la police, avec des crissements de pneus, dans l'une de ses flottes de supercars.

Pendant une décennie, le multimillionnaire aurait dirigé le groupe de cybercriminalité le plus nuisible au monde - Evil Corp., qui porte bien son nom. Il a ciblé des milliers de Britanniques et volé leurs économies en piratant leurs coordonnées bancaires.

Yakubets, qui a travaillé pour l'agence de renseignement du FSB russe, vivrait comme un roi, dépensant plus de 250 000 £ lors de son mariage.

LES CYBER PUISSANCES DU MAL

La cyber armée chinoise: 100 000 soldats ?

Les hackers d'Anthem

Fujie Wang est un autre pirate informatique très recherché, le seul membre identifié d'un groupe plus important de pirates informatiques ayant participé au piratage Anthem de 2014. Considéré comme membre d'une unité chinoise de cyberespionnage, Wang est toujours en fuite en Chine. Il a été officiellement inculpé plus tôt ce mois-ci.

Cyber-espionnage : des officiers de l'armée chinoise poursuivis par les États-Unis

ACTUALITE > INTERNATIONAL Par Anne-Laure Frémont | Mis à jour le 20/05/2014 à 08:26 | Publié le 19/05/2014 à 18:28

L'AUTEUR
SUR LE MÊME SUJET
RÉAGIR (115)
PARTAGER
IMPRIMER

LA NOUVELLE CYBERGUERRE MONDIALE

LES CYBER PUISSANCES DU MAL
La cyber armée iranienne

En février 2019, les États-Unis ont inculpé quatre ressortissants iraniens pour conspiration avec un ancien agent de renseignements de l'armée de l'air américain qui s'était rendu en Iran en 2013. Le groupe a utilisé les renseignements fournis par l'agent de l'US Air Force pour lancer des attaques de phishing par courrier électronique et par les médias sociaux.

Behzad Mesri, l'un des quatre pirates informatiques, avait déjà été accusé en novembre 2017 d'avoir piraté la chaîne HBO et d'avoir diffusé des épisodes et des scripts inédits de plusieurs séries télévisées, notamment de la série Game of Thrones diffusée sur HBO.

Identifié en mars 2018, ce groupe de pirates informatiques parrainé par l'État iranien a été accusé du piratage des réseaux de 320 universités à travers le monde. Le groupe était également connu sous le nom de Cobalt Dickens ou Silent Librarian dans les rapports de diverses entreprises de cybersécurité, et a poursuivi ses activités de piratage informatique malgré les accusations américaines.

LES CYBER PUISSANCES DU MAL

La cyber armée nord coréenne

North Korea 'launched cyber-attack on Pfizer for COVID-19 jab data'

Phil Taylor

February 16, 2021

A news agency is claiming that North Korea launched a cyber-attack on Pfizer in a bid to steal information about its BioNTech-partnered COVID-19 vaccine, citing South Korea's National Intelligence Service (NIS).

La Corée du Nord a volé des milliards d'euros en lançant des cyber-attaques

Selon un rapport des Nations Unies, deux milliards d'euros ont été dérobé au moyen de cyber-attaques lancées sur des banques et des bourses pour crypto-monnaies.

Mis en ligne le 8/08/2019 à 13:04

Kim Jong Un, le leader Nord Coréen, célébrant le lancement d'un missile le 7 Aout 2019 - KCNA/UPI

LA CYBER IGNORANCE ??

TOUTE L'ACTUALITÉ / SÉCURITÉ / DONNÉES PERSONNELLES

Les données de 1,4 million de patients subtilisées à l'AP-HP

Jacques Cheminat , publié le 16 Septembre 2021

Suite à une cyberattaque pendant l'été, des pirates ont réussi à dérober des données de 1,4 million de personnes ayant réalisé des tests Covid à la mi-2020. Une plainte a été déposée et la Cnil notifiée.

Les données de dépistage Covid de 1,4 million de personnes ont été dérobées à l'AP-HP. (Crédit Photo : Kollinger/Pixabay)

Comment réagir à cette menace mortelle de la Cyber coercition

une volonté affichée

une organisation efficace

un arsenal adapté

et une industrie innovante

La cyber dissuasion ??

USA: une politique cyber agressive de riposte une cyber dissuasion à plusieurs couches

Cybersécurité : attaqués, les Etats-Unis se mettent en ordre de bataille

Avec la multiplication d'attaques informatiques contre les agences gouvernementales, Microsoft ou l'oléoduc Colonial, Joe Biden fait de la cybersécurité l'une de ses priorités. Il a créé plusieurs postes pour renforcer la riposte fédérale. Un rapport du Congrès publié l'an dernier recommande une « cyberdissuasion à plusieurs couches ».

Lire plus tard | Air Défense | Partager | Commenter

Un poste de directeur national cyber, directement rattaché au bureau exécutif du président, a été créé. (Shutterstock)

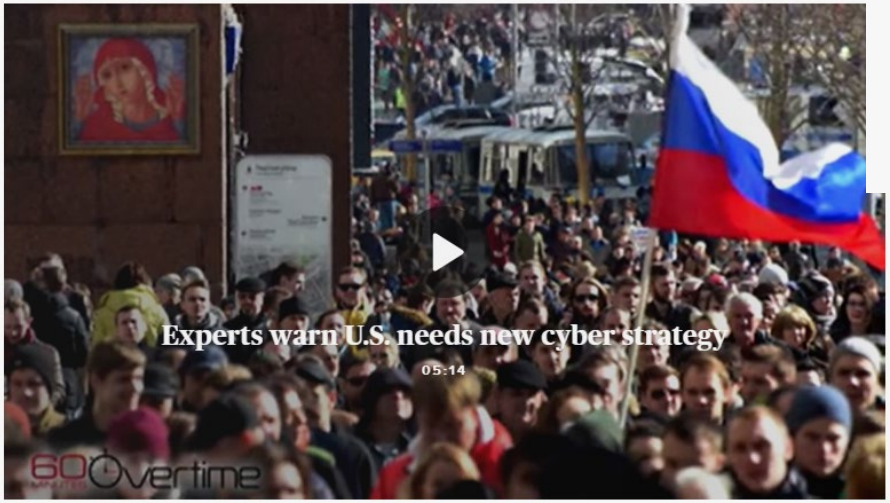
USA: une cyber dissuasion à plusieurs couches

Un directeur National Cyber, ex N2 NSA

HOW U.S. CYBER POLICY CHANGED AFTER SOLARWINDS

The Biden Administration imposed sanctions on Russia, ordered new cybersecurity standards for federal contracts with software companies, an chose the nation's first National Cyber Director.

2021 JUL 04 BY WILL CROXTON FACEBOOK TWITTER REDDIT FLIPBOARD



Chris Inglis, confirmed by the Senate to become the nation's first National Cyber Director, testifies during his confirmation hearing in Washington, DC. / GETTY IMAGES

USA: une cyber dissuasion à plusieurs couches

Une experte de la NSA Cyber Conseiller du président

Anne Neuberger

Anne Neuberger was named Deputy National Security Advisor for Cybersecurity and Emerging Technology by the Biden Administration in early 2021. Neuberger joined the NSA more than a decade ago and served as the agency's director of cybersecurity since 2019.

Prior to her assignment as Deputy National Security Advisor, Anne served as the Chief Risk Officer and the Director of NSA's Commercial Solutions Center, responsible for NSA's interface and partnerships with the private sector. Prior to that, she served as Special Assistant to the Director, NSA, building a deep and effective partnership, the Enduring Security Framework, between leading companies, the Departments of Defense, Homeland Security, NIST and NSA, on initiatives across a broad set of technical and policy areas. In this capacity, Anne also led the Department of Defense's Defense Industrial Base Pilot, defining the first policy and legal framework for government sharing of classified signatures and indicators with Internet Service Providers. Prior to ESF, Anne served as a leader of the U.S. Cyber Command Implementation Team which led the planning and standup of USCYBERCOM.

USA: une cyber dissuasion à plusieurs couches

Une ex de la NSA à la CISA

Jen Easterly Sworn in as New CISA Director

By **Homeland Security Today** August 11, 2021

Share | Facebook | Twitter | Linkedin | Email

New Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly is sworn in at CISA Headquarters in Arlington, Va., on Aug. 9, 2021. (DHS photo)

Jen Easterly was sworn in Monday to lead the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security.

Easterly was a managing director at Morgan Stanley, serving as global head of the firm's Fusion Resilience Center, and a senior fellow at New America's International Security program. After her NSA role from 2011-2013, she served on the National Security Council as special assistant to the president and senior director for counterterrorism.

USA: une cyber dissuasion à plusieurs couches

Mobilisation des GAFAM

INTERNATIONAL - ÉTATS-UNIS

Favoris Partage

Cybersécurité : reçus par Biden, les leaders de la tech annoncent des formations et des investissements

Les dirigeants de Google, Amazon, Apple et Microsoft se sont rendus mercredi à la Maison Blanche pour une réunion d'urgence sur le sujet avec le président américain.

Le Monde avec AFP

Publié le 26 août 2021 à 00h08 - Mis à jour le 26 août 2021 à 08h33 - Lecture 3 min.

Le président américain, Joe Biden, s'exprime lors d'une réunion sur la cybersécurité dans la salle est de la Maison Blanche, à Washington, mercredi 25 août 2021. EVAN VUCCI / AP

Le président américain Joe Biden a réuni, mercredi 25 août à la Maison Blanche, des ministres, les patrons des géants de la tech et de grandes sociétés pour une réunion d'urgence sur la cybersécurité, après une vague d'attaques informatiques qui a mis en lumière des vulnérabilités majeures.

USA: une cyber dissuasion à plusieurs couches

Mobilisation de MICROSOFT 20 Milliards

TECHNOLOGY EXECUTIVE COUNCIL

Microsoft has a $20 billion hacking plan, but cybersecurity has a big spending problem

PUBLISHED WED, SEP 8 2021-10:04 AM EDT | UPDATED WED, SEP 8 2021-1:29 PM EDT

Eric Rosenbaum
@ERPROSE

SHARE

KEY POINTS

- Microsoft is quadrupling its cybersecurity investment to $20 billion over the next five years.
- One of the reasons for the big investment cited by Microsoft president Brad Smith in a CNBC interview this week speaks to a Catch-22 in the cyber arms race: the increased spending in recent years by public and private enterprises hasn't resulted in better protection against criminal hackers.
- The shortage of workers skilled in cybersecurity is one of the factors that has led to a situation in which companies are paying for products that in many cases they aren't even using.

In this article MSFT -0.27 (-0.09%)

De la cybercoercition vers une guerre physique ?

Joe Biden prévient : si une «véritable guerre» éclate avec une autre grande puissance, «ce sera à cause d'une cyberattaque»

Par Le Figaro avec AFP
Publié le 27/07/2021 à 23:59, mis à jour le 30/07/2021 à 14:39

Le président américain Joe Biden a qualifié son homologue russe Vladimir Poutine de «dangereux». *EVELYN HOCKSTEIN / REUTERS*

Le président américain a également reproché mardi à la Russie de chercher à perturber les élections législatives de 2022 aux États-Unis.

Joe Biden joue les augures à l'ère du tout numérique. *«Si nous nous retrouvons en guerre, dans une véritable guerre armée, avec une autre grande puissance, ce sera à cause d'une cyberattaque»*, a-t-il assuré mardi 27 juillet, lors d'une allocution devant les services de renseignement.

UK: Création d'une national Cyber force , passer de la défensive à l'offensive

Britain

Use the force

Britain puts a new offensive cyber force at the heart of its defence

The National Cyber Force of soldiers and spies has been quietly hacking away, but it must tread carefully

UK: Création d'une national Cyber force , passer de la défensive à l'offensive

What Will the Force Entail?

On Thursday 19th November 2020, the UK Prime Minister announced a new partnership: the National Cyber Force (NCF). This new body is the result of cooperation between the Ministry of Defence and Government and Communications Headquarters (GCHQ). MI6 and the Defence, Science and Technology Laboratory will also contribute.

The four organisations will collaborate under one unified command for the first time. The Ministry of Defence's official tagline for the NCF is, "A Defence and Intelligence Partnership", to emphasize the fact that there is no other organization like it anywhere else on the globe, to date.

UK: Création d'une national Cyber force , passer de la défensive à l'offensive

The Guiding Objectives of the Taskforce

The principal objective of the NCF will be to degrade, disrupt and even destroy communications systems of those that pose a security threat. The Force will monitor both local and global cybersecurity threats. The organisation's remit will also encompass the support of ongoing military operations.

The organization, reportedly secretly launched in April 2020, has the goal of disrupting the operations of national security threats. For example, via hacking enemy weapons systems and disrupting hostile states' servers.

Another reported tactic the NCF will use is to take a behavioural science approach in an attempt to communicate with attackers to deterand steer them away from their planned attacks. These tactics are in contrast to the pre-existing, more *defensive,* bodies such as the National Cyber Security Centre (NCSC), whose main function is to help the public sector, businesses and the public to respond to, and recover from, cyber incidents.

•France: Une stratégie nationale et globale pour créer une capacité de riposte

OPINIONS • DÉFENSE

« Qu'elles soient étatiques ou criminelles, les intrusions informatiques doivent être combattues par une stratégie nationale et globale »

TRIBUNE

Bernard Barbier
Ancien directeur technique de la DGSE

Jean-Louis Gergorin
Ancien chef du Centre d'analyse et de prévision du Quai d'Orsay

Amiral Edouard Guillaud
Ancien chef d'état-major des armées

La « cybercoercition » implique de combiner renseignement, protection, action internationale et capacité de riposte, soulignent, dans une tribune au « Monde », trois anciens hauts responsables de la défense française.

•France: Une stratégie d'anticoercition, intégrée et globale

renseignement, protection, action internationale et capacité de riposte.

Dans ce contexte, la cybercoercition, qu'elle soit étatique ou criminelle, doit être combattue par une stratégie nationale d'anticoercition intégrée et globale. Celle-ci comporterait quatre volets étroitement liés: renseignement, protection, action internationale et capacité de riposte.

-Le renseignement doit identifier les responsables des attaques et les signatures techniques de celles-ci. Pour ce faire, la coopération entre services de renseignement officiels, agences de cybersécurité et entreprises spécialisées de confiance est primordiale.

-**La protection est une condition nécessaire mais non suffisante de la sécurité**. A cet égard l'attaque Sunburst est une alerte majeure sur la nécessité de ne plus s'en remettre aux seules certifications initiales des logiciels. Des mécanismes de contrôle des mises à jour doivent être mis en place. Enfin il est anormal que la France, exportatrice de cerveaux numériques, n'arrive pas à mieux stimuler la création et le développement d'entreprises de logiciels de cybersécurité, mettant fin au duopole américano-israélien dominant le marché européen.

•France: Une stratégie d'anticoercition, intégrée et globale

renseignement, protection, action internationale et capacité de riposte.

-**Enfin la doctrine française de cyberdéfense doit prévoir la possibilité de riposte proportionnée à toute attaque contre des infrastructures jugées essentielles aussi bien civiles que militaires**.

Sous l'impulsion de Thierry Breton la Commission européenne vient d'annoncer une nouvelle stratégie cyber incluant la cyberdéfense.

Pour lutter au bon niveau, des objectifs ambitieux et atteignables doivent être fixés. Vouloir éradiquer la cyber criminalité est illusoire : la réduire est à notre portée. La lutte cyber pourrait s'inspirer de l'opération ATALANTE contre la piraterie menée dans l'océan Indien depuis 2008, qui a vu l'Union européenne s'appuyer sur un premier pays, la France en l'espèce, pour allier rapidité et efficacité.

Les ripostes d'anticoercition pourraient être effectuées par le ComCyber ou la DGSE, ou par une équipe intégrée commune comme en Grande Bretagne, à l'échelon national ou en coopération avec des alliés. Sans l'évolution doctrinale déjà évoquée sur le caractère global de la cyberdéfense il n'y aura aucun effet dissuasif et rien n'empêchera la répétition de plus en plus grave de ce que le CHU de Rouen a subi en novembre 2019.

•France: Une stratégie d'anticoercition, intégrée et globale

renseignement, protection, action internationale et capacité de riposte.

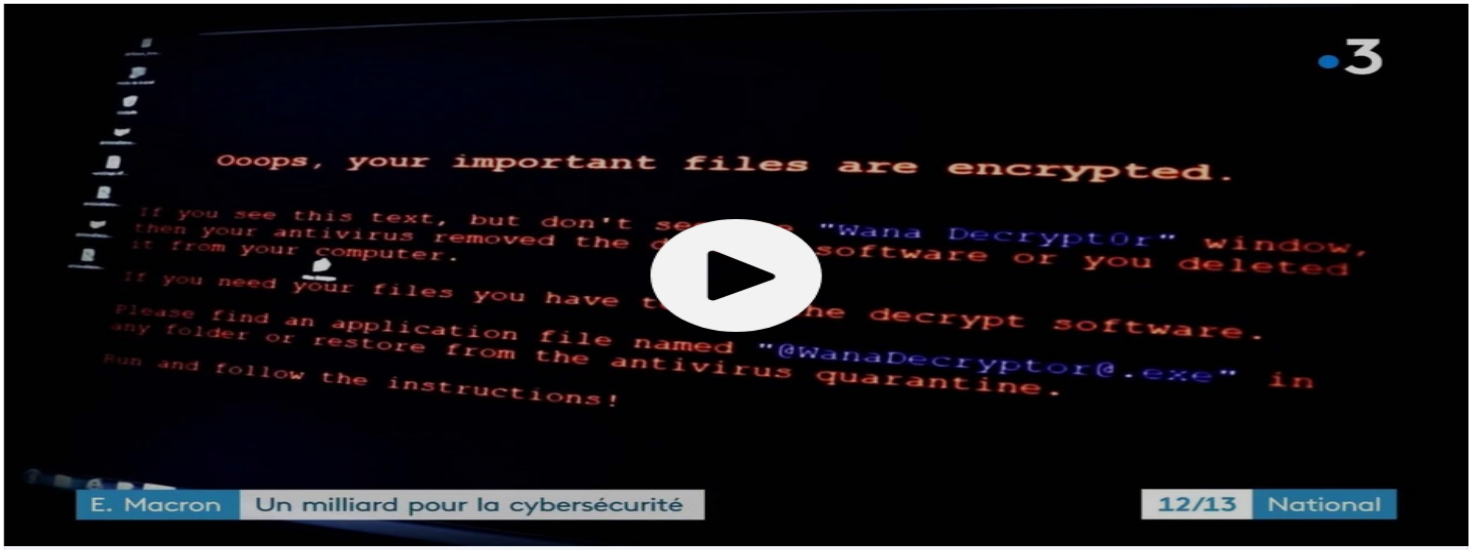
Face aux ruptures que représentent la croissance exponentielle des rançongiciels et l'opération « SUNBURST », notre pays doit très rapidement engager une réflexion stratégique et sortir de la logique incrémentale qui n'est plus adaptée au contexte.

Plus que jamais, il nous parait indispensable que le Président de la République puisse s'appuyer sur un **Coordonnateur National Cyber (CNC)** à l'instar du Coordinateur National du Renseignement de de Lutte contre le Terrorisme (CNRLT) qui a montré son efficacité.

•Réponse de la France : un plan d'investissement de 1 milliards euros

Cybersécurité : Emmanuel Macron annonce un plan global à 1 milliard d'euros

Publié le 18/02/2021 17:38 Mis à jour le 18/02/2021 17:40 Durée de la vidéo : 2 min.



D.Schlienger, T.Grosse, C. Baume, M. Le Rue - France 3
France Télévisions

12/13
Édition du jeudi 18 février 2021

Alors que deux hôpitaux de Dax (Landes) et de Villefranche-sur-Saône (Rhône) ont récemment été victimes de cyber-attaques, Emmanuel Macron a réagi en annonçant, jeudi 18 février 2021, un plan de lutte dédié à la cybersécurité à 1 milliard d'euros.

- Apprendre à gérer la guerre cyber
- une volonté affichée, accepter la notion de rapport de force

OPINIONS • CYBERCRIMINALITÉ

« L'affaire Pegasus montre parfaitement les faiblesses de l'Europe en matière de cyberagressions »

TRIBUNE

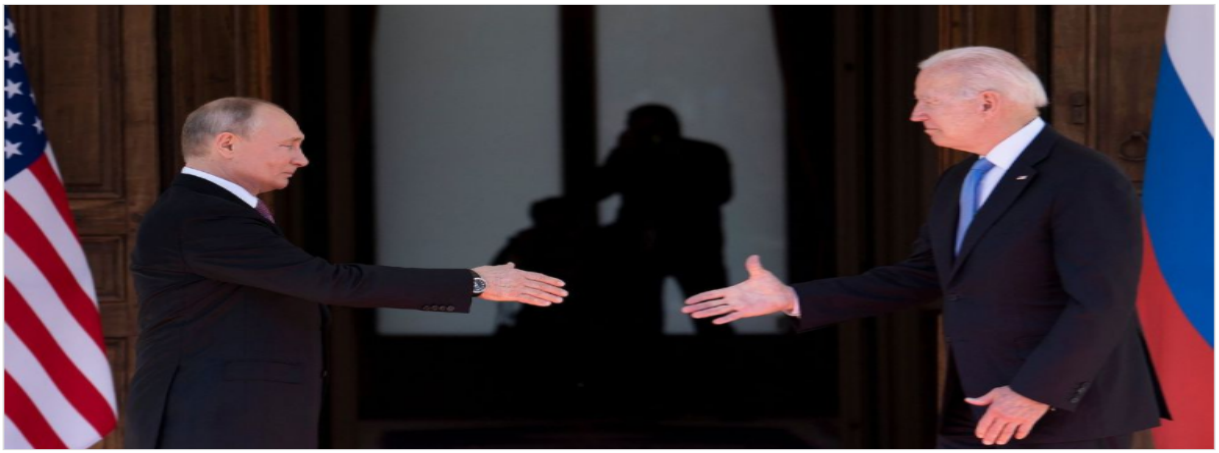
Collectif

L'Union européenne et la France doivent accepter la notion de rapport de force et oser des mesures de rétorsion, estiment Bernard Barbier, ancien directeur technique de la DGSE, Jean-Louis Gergorin, ancien chef du Centre d'analyse et de prévision du Quai d'Orsay et l'amiral Edouard Guillaud, ancien chef d'état-major des armées, dans une tribune au « Monde ».

Les éléments clés de succès, apprendre à gérer la guerre cyber et disposer de l'arsenal adapté

Attaques informatiques : l'urgence d'une convention de Genève du cyberespace

Devant la multiplication des cyberattaques, un accord international de protection dans l'univers du numérique devient impératif.



Le président américain Joe Biden et son homologue russe se serrent la main au début de leur sommet à Genève, le 16 juin 2021.
afp.com/Brendan Smialowski

Par Emmanuel Paquette

Publié le 23/08/2021 à 17:54, mis à jour le 24/08/2021 à 10:48

— Dans l'hebdo du 26 Août

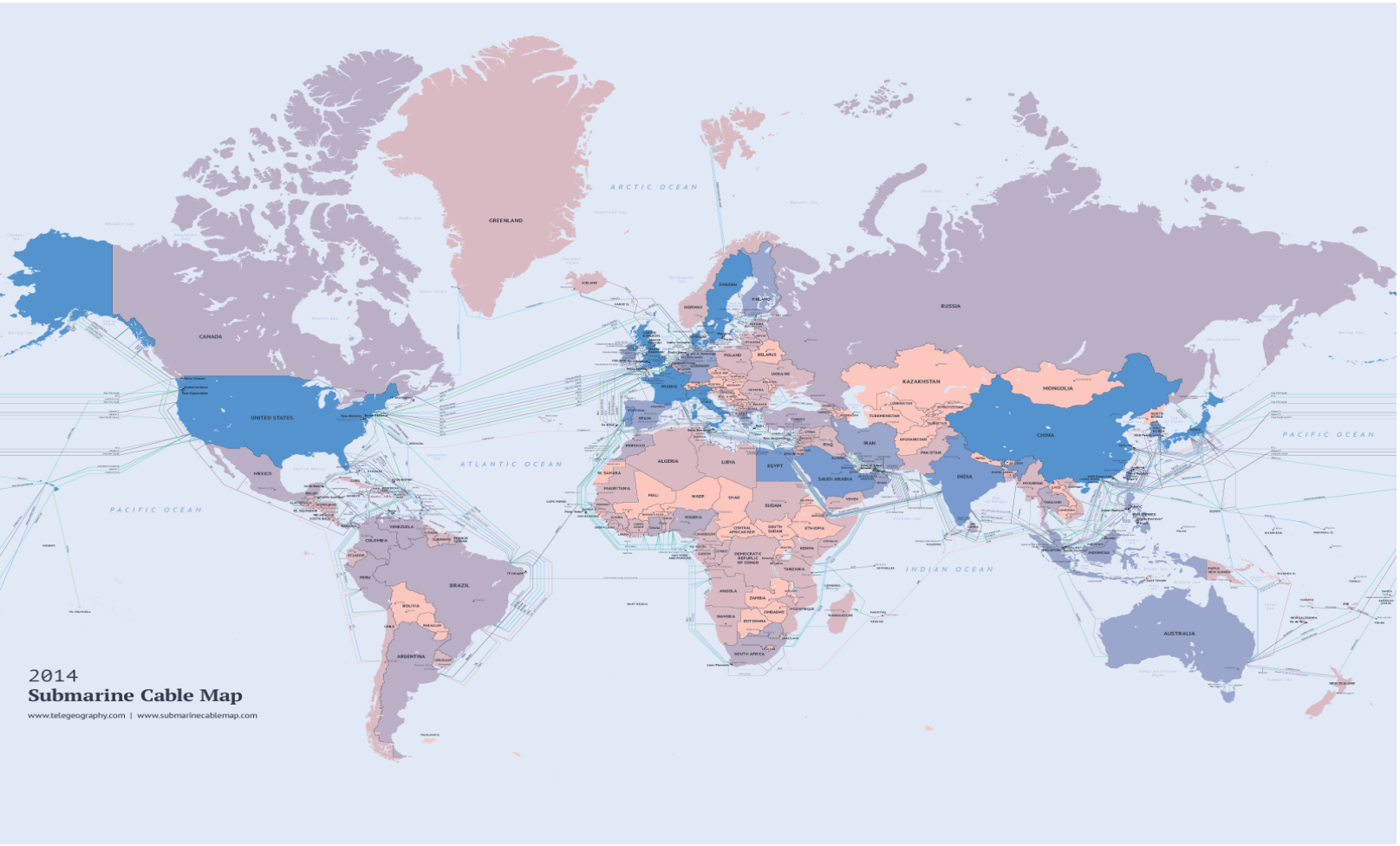
High-Tech

Écouter cet article sur l'application

Le face-à-face électrique s'est tenu en terrain neutre, en Suisse, dans la ville de Genève. Le 16 juin dernier, le président américain Joe Biden a rencontré son homologue russe, Vladimir Poutine, pour lui intimer d'agir contre les récentes cyberattaques en provenance, selon lui, de Russie. Si rien n'est fait, des "mesures nécessaires" pour se défendre seront prises, a même menacé l'hôte de la Maison-Blanche.

LA CYBER PUISSANCE AMERICAINE

Ne pas oublier SNOWDEN



STORMBREW, FAIRVIEW, BLARNEY, OAKSTAR….25 centres de collecte de câbles sous marins

LA CYBER PUISSANCE AMERICAINE

NEVER FORGET

EEI : H

EEI Classification : SECRET//NOFORN

Originator EEI Classification : SECRET//REL TO USA, AUS, CAN, GBR, NZL

EEI Title : (U//FOUO) Foreign Contracts/Feasibility Studies/Negotiations

Question(s) :

1. (S//REL TO USA, AUS, CAN, GBR, NZL) Report impending French contract proposals or feasibility studies and negotiations for international sales or investments in major projects or systems of significant interest to the foreign host country or $200 million or more in sales and/or services, including financing information or projects of high interest including:

A. Information and telecommunications facilities networks and technology?

B. Electric power, natural gas, and oil facilities and infrastructure to include nuclear power and renewable energy generation?

C. Transportation infrastructure and technology to include ports, airports, high-speed rail, and subways?

D. Environmental technologies used domestically and for export?

E. Health care infrastructure, services, and technologies, including biotechnology developments?

NOS AMIS BRITANNIQUES:

MALHEUR AUX MAUVAIS

NCSC : « Mon travail, ce n'est pas de mettre fin au cybercrime. C'est de l'envoyer en France »

Sécurité : *Le NCSC, agence britannique dédiée à la cybersécurité, dévoile ses plans pour protéger les citoyens britanniques contre les attaques informatiques : protéger la mère patrie et pousser mécaniquement les cybercriminels à s'intéresser aux pays voisins*

Par Louis Adam | Modifié le vendredi 12 oct. 2018 à 16:53

Suivre @zdnetfr

« Mon travail, ce n'est pas de mettre fin au cybercrime. C'est de l'envoyer en France » : on peut dire que Ian Levy le directeur technique du NCSC a le sens de la formule. Comme le rapporte ZDNet.com, celui-ci s'exprimait hier à l'occasion d'une keynote organisée par l'association australienne de Cybersécurité. Il y revenait notamment sur son rôle au sein du NCSC, l'équivalent britannique de l'Anssi placé sous la coupe du GCHQ, et sur l'évolution des plans mis en place pour protéger les citoyens britanniques des attaques.