Guerre économique et économie de Guerre

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)

SOMMAIRE

La situation actuelle sur le font RUSSIE-UKRAINE

Les actions préventives des USA

Europe et France

Guerre de l'Information: de l'Ukraine au Mali

Cyber espionnage

Guerre économique et économie de Guerre

La situation actuelle sur le font RUSSIE-UKRAINE

Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds

A new study by Microsoft shows that Russian cyberattacks often happened within days or even hours of missile strikes.

Give this article 59

President Vladimir V. Putin of Russia on Wednesday. His country used hackers to conduct hundreds of subtle cyberattacks in Ukraine, many timed to coincide with incoming missile or ground attacks, according to a new report. Alexandr Demyanchuk/EPA, via Sputnik

Cyberattaque : la Russie a piraté un réseau de satellites juste avant l'invasion de l'Ukraine

En visant ce réseau de satellites, le gouvernement russe a déclenché des pannes dans toute l'Europe, quelques heures seulement avant que la Russie ne lance son invasion de l'Ukraine.

Par Valentin Cimino - @ciminix
Publié le 11 mai 2022 à 09h37

Photographie : NASA

Les États-Unis, le Royaume-Uni et l'Union européenne accusent la Russie **d'être responsable d'une cyberattaque sur le réseau de satellites KA-SAT**, exploité par la société Viasat. Ce piratage a eu lieu juste avant l'invasion de l'Ukraine par la Russie, pour saboter les communications des ukrainiens.

À lire aussi

Guerre économique et économie de Guerre

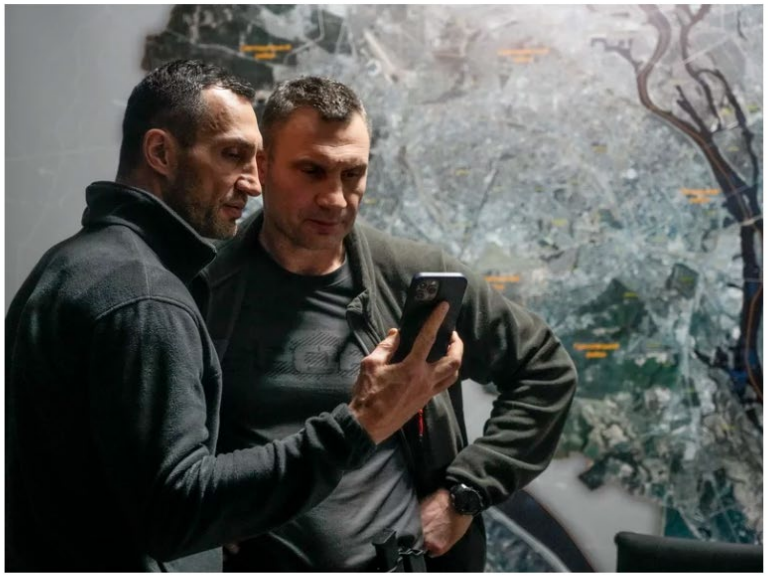
La situation actuelle sur le font RUSSIE-UKRAINE

How does Ukraine keep intercepting Russian military communications?

April 26, 2022 · 1:34 PM ET
Heard on All Things Considered

GREG MYRE

4-Minute Listen + PLAYLIST



Kyiv Mayor Vitali Klitschko (right) and his brother Wladimir Klitschko check a phone at city hall on Feb. 27. When Russia invaded Ukraine, many expected Moscow to knock out the Ukrainian communications network. But Ukrainian systems, for both civilians and the military, continue to function. Ukraine, meanwhile, has regularly intercepted Russian military communications.

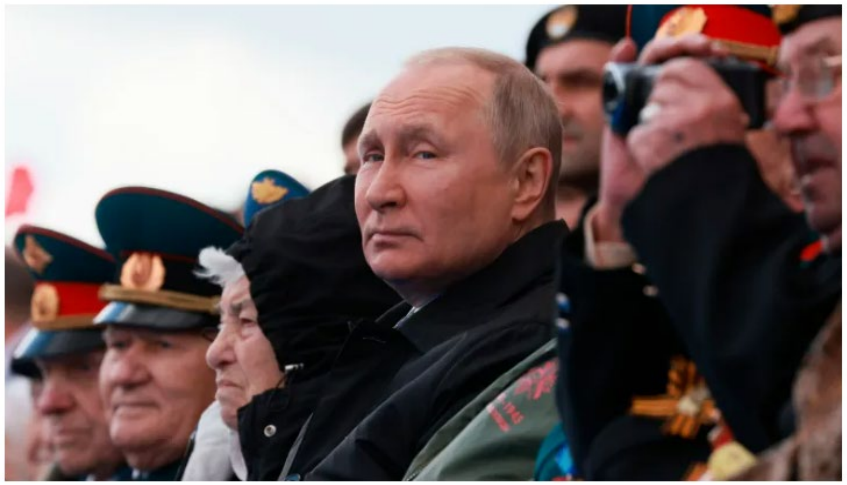
Efrem Lukatsky/AP

Politics

Russia's dreaded cyberwarriors seem to be struggling in Ukraine

Russia's hackers — like its military — may not be quite as fearsome as the world thought

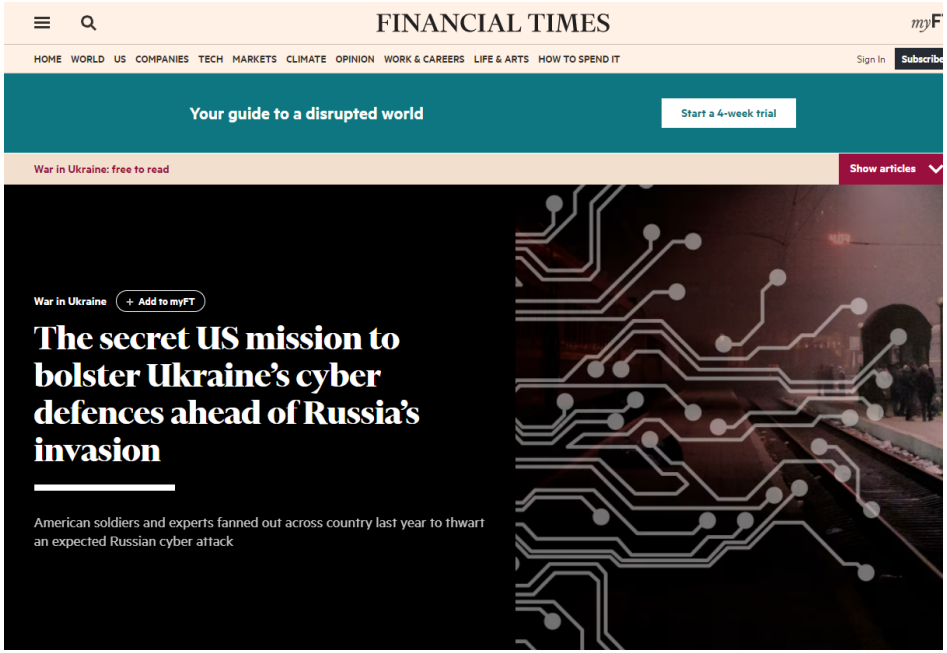
Evan Dyer · CBC News · Posted: May 22, 2022 4:00 AM ET | Last Updated: May 22



Russian President Vladimir Putin looks on during the Victory Day military parade in Moscow on May 9, 2022. Russia's celebration was marred by the news that its online TV schedule page had been hacked — another sign that Russia's cyberwar in Ukraine hasn't been going all that well. (Mikhail Metzel/Sputnik/Kremlin Pool Photo/The Associated Press)

Guerre économique et économie de Guerre

Les actions préventives des USA



Cyber

US Cyber Command reinforces Ukraine and allies amid Russian onslaught

By Colin Demarest

Thursday, Apr 7

U.S. Cyber Command head Gen. Paul Nakasone arrives for a Senate Armed Services hearing on Capitol Hill in Washington, Tuesday, April 5, 2022. (AP Photo/Andrew Harnik)

WASHINGTON — U.S. Cyber Command has played a pivotal role in shielding networks and critical infrastructure stateside and abroad in the run up to and during Russia's attack on Ukraine, its leader told Congress this week.

US Cyber Chief Sees More Attacks in Russian Ukraine Playbook

- Attacks are likely to 'continue apace' as war drags on
- Cyber Director Inglis in Singapore as part of a regional tour

Chris Inglis *Photographer: Drew Angerer/Getty Images*

By Jamie Tarabay and Philip Heijmans
13 mai 2022, 05:02 UTC+2 *Updated on 13 mai 2022, 05:23 UTC+2*

White House Cyber Director Chris Inglis said on Friday he expects Russia's use of disruptive cyber attacks to continue so long as there is war in Ukraine.

Ukraine war: Don't underestimate Russia cyber-threat, warns US

By Gordon Corera
Security correspondent, BBC News

11 May

Russia-Ukraine war

There has been a sustained cyber-conflict over Ukraine which could still escalate, a senior US intelligence official has told the BBC.

Despite warnings, major cyber-attacks on the West have so far not materialised.

But Russia shouldn't be underestimated, Rob Joyce, director of cyber-security at the National Security Agency said.

Guerre économique et économie de Guerre

Europe et France

Guerre en Ukraine : l'Europe accuse la Russie d'avoir paralysé des satellites pour préparer l'invasion

Lecture 1 min

Accueil • International • Europe • Guerre En Ukraine : Actualités Et Directs

L'invasion militaire a été précédé par une cyberattaque, une heure avant. © Crédit photo : YASUYOSHI CHIBA/AFP

Publié le 10/05/2022 à 14h56

S'ABONNER

C'est la première fois que l'Union européenne met clairement en accusation le Kremlin pour ces cyberattaques le jour de l'invasion, le 24 février

L'Union européenne a accusé mardi les autorités russes d'avoir mené une cyberattaque contre un réseau de satellites une heure avant l'invasion de l'Ukraine, le 24 février dernier, afin de préparer le terrain à son assaut.

Cyberattaque : les terminaux pétroliers de plusieurs ports visés en Allemagne, Pays-Bas et Belgique

Sont notamment concernés les ports de Hambourg, Gand ou Anvers, avec pour conséquence la perturbation des livraisons d'énergie.

Plusieurs grands ports européens ont été touchés par cette cyberattaque (Photo d'illustration). AFP/EMMANUEL DUNAND

Guerre économique et économie de Guerre

Europe et France: Il y a 40 ans, La crise des euro missiles
Dissuasion nucléaire-cyber dissuasion

Le monde au bord de la crise nucléaire

L'abandon des grands traités de réduction et d'élimination des armes nucléaires conclus entre la Russie et les Etats-Unis fait peser une grave menace sur le monde.

Lire plus tard | Éditos & Analyses | Partager | Commenter

Le monde se rapproche dangereusement d'une situation de crise nucléaire, comme ce fut le cas à Cuba dans les années 1960 ou en Europe avec l'installation de missiles soviétiques SS-20 et de Pershing américains. (Shutterstock)

Face à la crise des Euromissiles : la politique de dissuasion française

16 novembre 1983

La dissuasion nucléaire française, totalement autonome, c'est l'assurance ultime, c'est une arme de non emploi

La recherche scientifique, la conception et la fabrication des têtes nucléaires est de la responsabilité d'un acteur unique: Le CEA

POURQUOI AVONS-NOUS PERDU NOTRE AUTONOMIE ?
LA CYBER-DISSUASION FRANCAISE PEUT-ELLE EXISTER?

Pas de politique européenne de cyber dissuasion
Une organisation Française dispersée

SOCIÉTÉ • POLICE

Sélections | Partage

Guerre des polices dans le cyberespace

Face à la montée en puissance de la cyberdélinquance, le ministère de l'intérieur envisageait la création d'une structure unique confiée à la gendarmerie. Les réticences de la police l'ont conduit à modifier son projet.

Par Antoine Albertini

Publié le 21 janvier 2022 à 01h48 - Mis à jour le 21 janvier 2022 à 10h58 - Lecture 7 min.

Article réservé aux abonnés

Le plan était ambitieux, il devait même figurer parmi les innovations de la loi de programmation du ministère de l'intérieur, grand œuvre de Gérald Darmanin en matière de sécurité : créer un grand « service à compétence nationale » de lutte contre la cyberdélinquance. Las.

La traditionnelle guerre des polices a eu raison du projet, qui devait échoir aux gendarmes, et le ministre a dû revoir ses ambitions à la baisse. *« Le cyber est un nouveau territoire de délinquance qui impacte chaque Français, chaque entreprise, chaque administration,* assure aujourd'hui Gérald Darmanin. *Cela n'aurait eu aucun sens de le réserver à une force, ce serait comme dire : les policiers sont désormais les seuls à avoir des voitures. »*

Face aux cybermenaces, les gendarmes se mettent en ordre de bataille

Par Delphine Dechaux le 10.09.2021 à 15h02

Lecture 4 min.

Face à l'explosion des cyberattaques, la gendarmerie s'est réorganisée sous le pavillon unique du ComCyberGend (Commandement de la gendarmerie dans le cyberespace). Un premier jalon avant la création d'un service cyber mixte réunissant police et gendarmerie. Challenges a rencontré le général Boget à la tête de cette nouvelle structure, unifiée et simplifiée.

Face à l'explosion des cybermenaces, la gendarmerie se réorganise sous un commandement unifié, le ComCyberGen, qui intégrera les policiers.

KACPER PEMPEL

Guerre économique et économie de Guerre

UK: Une vraie stratégie de Cyber Dissuasion

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

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.

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.

La guerre de l'information est devenue globale et totale: La France visée par la Russie en Afrique

lefigaro.fr

Moscou dénonce la politique «coloniale» de Paris au Mali

Le chef de la diplomatie russe Sergueï Lavrov a dénoncé vendredi 20 mai la «mentalité coloniale» de Paris et de l'Europe au Mali, en receva...

INFO

sy @KalySy · 21 mai

FAMAS:les mercenaires ivoiriens suivis et bombardésLes déplacement des commandos ivoiriens filmés par satellite depuis la forêt de Séguéla ont été frappé par les FAMAS.Vive le **Mali**

Ce sont des équipements fournis par la Russie qui ont permis de réaliser cette opération.

C-yapi

4 15 75

La guerre de l'information est devenue globale et totale: La France visée par la Russie en Afrique

Mali : dans la guerre de l'information, l'armée française réplique et accuse le Groupe Wagner

Les militaires français ont filmé ce qu'ils affirment être des mercenaires russes en train d'enterrer des corps près de la base de Gossi, dans le nord du Mali.

Ukraine : de Moscou, Pékin ou Téhéran, les 1001 facettes de la guerre de l'information

Publié le : 19/05/2022 - 18:03

Mandiant, une société de cybersécurité américaine, a fait un premier bilan de la guerre d'information autour du conflit en Ukraine. © Studio graphique France Médias Monde

Texte par : Sébastian SEIBT Suivre 7 mn

L'étendue des efforts des groupes prorusses pour répandre la désinformation autour de la guerre en Ukraine est dévoilée dans un rapport de la société de cybersécurité Mandiant, consulté par France 24. Mais le conflit a aussi été récupéré par des cyberagents chinois et iraniens.

INFO OU INTOX

Associer nazisme et Ukraine, un leitmotiv dans la désinformation

Publié le : 17/05/2022 - 21:49

INFO OU INTOX © France 24

2.1. L'espionnage reste la première finalité poursuivie, notamment en France

La menace d'espionnage stratégique demeure une constante à prendre en compte; elle touche autant les acteurs institutionnels que privés. La France est particulièrement ciblée par cette menace comme en témoignent les campagnes d'attaques mettant en œuvre les modes opératoires Sandworm [16], Nobelium [17] ou encore APT31 [10] en 2020-2021. **En 2021, sur les 17 opérations de cyberdéfense traitées par l'ANSSI, 14 étaient liées à des opérations d'espionnage informatique, impliquant pour 9 d'entre elles des modes opératoires réputés chinois. De même, sur 8 incidents majeurs, 5 concernent des MOA réputés chinois.**

Le détournement de cadres juridiques étrangers liés à la cybersécurité peut également faciliter ces actions d'espionnage visant à capter des données à caractère personnel des citoyens français et/ou des données appartenant à des entreprises françaises implantées à l'étranger. Si les dispositifs législatifs relatifs à la cybersécurité se multiplient dans le monde, plusieurs cas de détournement à des fins d'espionnage de dispositifs légaux sans lien avec la cybersécurité ont été rapportés ou soupçonnés. Ainsi certaines versions du logiciel GoldenTax, imposé en Chine, ont embarqué une porte dérobée permettant un accès furtif aux systèmes d'information de plusieurs entreprises [18]. De plus, l'extraterritorialité de certaines législations étrangères en matière de sécurité nationale [3], une notion

3. ITAR, FISA ou le Cloud Act par exemple, ou encore loi sur le renseignement en république Populaire de Chine.

Guerre économique et économie de Guerre

Cyber espionnage: pas d'amis

La Chine a lancé une vaste opération de cyber-espionnage en Europe

PAR FLORIAN BAYARD
LE 04/05/2022

La Chine a déployé une importante opération de cyber-espionnage à l'encontre d'entreprises américaines, européennes et asiatiques. Dans le cadre de l'attaque, des hackers chinois ont volé des informations confidentielles en exploitant des failles de Windows.

Cyberespionnage russe : l'UE hausse le ton

Josep Borell, le chef de la diplomatie européenne. / Photo AFP, Angela Weiss

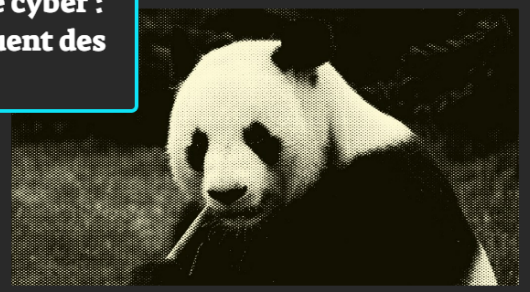
Publié le 28 avril 2022 à 13h01

>_ Cyberguerre ▪ Cybercriminalité

Il n'y a pas d'alliés dans le cyber : des pirates chinois attaquent des Russes

Pas d'amis dans la cyber.

Temps de lecture : 1 min



Bogdan Bodnar

Ghostwriter : l'Europe accuse la Russie de cyberespionnage

Une opération de piratage, nommée Ghostwriter, touche de nombreux États et individus de l'Union Européenne. La Russie est officiellement accusée d'en être à l'origine.

Par Grégoire Levy - @GregoireLevy
Publié le 27 septembre 2021 à 13h13

Ghostwriter désigne une opération de cyberespionnage touchant les membres de l'Union Européenne. Cette dernière accuse la Russie d'être à l'origine de l'opération. Image : Jefferson Santos/Unsplash.

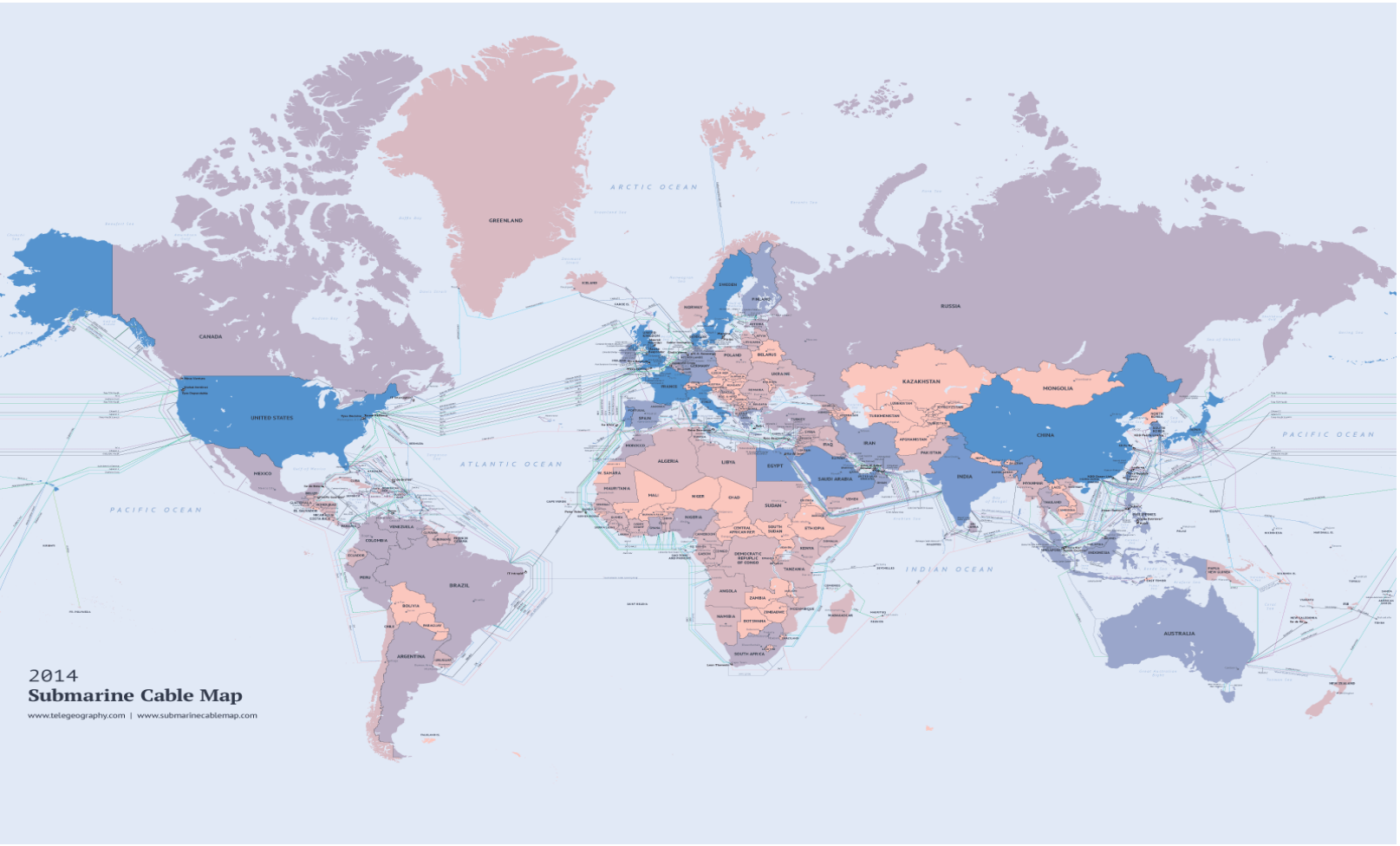
L'Union Européenne a officiellement incriminé la Russie de cyberespionnage, vendredi 24 septembre. Le gouvernement russe est accusé d'ingérence dans des élections de plusieurs États de l'UE, de piratage de comptes, et de vols de données.

À lire aussi

Guerre économique et économie de Guerre

LA CYBER PUISSANCE AMERICAINE

Ne pas oublier SNOWDEN



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

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?

Cybersecurity150.com

Hot 150 Cybersecurity Companies To Watch In 2021

Second annual list of pure-play vendors and service providers Press Release

– Steve Morgan, *Editor-in-Chief*

Sausalito, Calif. – Jan. 5, 2021

Thousands of startups have been formed over the past decade to focus on combating cybercrime, which is expected to cost the world $6 trillion annually in 2021 — up from $3 trillion in 2015.

The second annual list of the Hot 150, compiled by Cybersecurity Ventures, recognizes the most innovative companies in the cybersecurity market. The list consists of pure-play companies focused exclusively or primarily on cybersecurity. All companies earn their spot based on merit, there is no "pay-to-play," no cost to apply or to be listed.

Les valorisations en milliards de dollars

PALO ALTO: 48,4
FORTINET 46
CROWDSTRIKE 35
ZSCALER 32
OKTA 13
TENABLE 5
CYBER ARK 5,3
QUALYS 4,7
DARKTRACE 4

WALLIX 0.101