5. France

The French government has robust strategies for security in cyberspace, supported by mature institutions and regular budget infusions. France has a wide cyber-intelligence reach but keeps its cybersecurity functions organisationally separate from its intelligence community. In terms of digitisation of its society and economy, France is not one of the leaders among the world's developed countries, though its ICT sector has clear strengths. It has shown itself to be highly capable and innovative on cyber security, advocating a whole-of-society approach. It also favours regulation as a means of addressing cyber threats, exemplified by new laws on election interference and protecting critical national infrastructure. On the international stage France has promoted multilateralism on cyber issues. Its offensive cyber capability is mature but probably lags behind those of the United States and the United Kingdom. Its desire for national autonomy on key cyber capabilities denies France the potential gain from a more integrated approach with key allies, but as a result it is less dependent on them.

Strategy and doctrine

Until 2011, France's approach to issues of cyberspace security was based on a mix of technical security needs, commercial perspectives and military interests. It has since moved more decisively towards a model that gives precedence to a unified view of national security in cyberspace. There is a striking contrast between its early strategy documents and those that have emerged since 2018.

The theme of digital security was prominent in a 2008 defence white paper that noted the challenges posed by the rapid spread of information and ideas via new technology, including in the political arena.[1] This was the first time a French public-policy document had acknowledged cyber- and information-warfare threats, and expressed determination to counter them. This intention was reflected in the creation a year later of the National Cybersecurity Agency (ANSSI)[2] under the direction of the Secretariat-General for Defence and National Security (SGDSN).[3] The first national cybersecurity strategy, published in 2011, after government ministries had been targeted in cyber attacks,[4] explicitly declared France's ambition to be a global cyber power, if only in a defensive sense. A 2013 defence white paper mandated the creation of a national doctrine for responding to major cyber threats, consisting of a coordinated defensive posture mixed with a graduated response.[5] Importantly, the 2013 white paper also contained France's official recognition of cyberspace as a military operational domain, two years after the United States had done so and three years before NATO.

List of acronyms

ANSSI	National Cybersecurity Agency
CDSN	Defence and National Security Council
DGA	General Directorate for Armaments
DGSE	General Directorate for External Security
ICT	information and communications technology
MdA	Ministry of the Armed Forces
SGDSN	Secretariat-General for Defence and National Security
SOC	Security Operations Centre

At that time, France's security environment was beginning to change as the result of a series of security shocks: the Edward Snowden leaks in 2013; jihadist terrorism between 2012 and 2016; and major data breaches including the so-called 'Macron Leaks' (the leaking of emails from Emmanuel Macron's 2017 presidential-election campaign, linked to Russian political interference in favour of the National Front candidate, Marine Le Pen).[6] These events pushed France to adopt a whole-of-society approach and to give more attention to the threat of political interference, disinformation and extremist propaganda in defining its cyber strategies and policies.

The first strong indication of a major shift in cyber policy came in January 2017, when the Ministry of the Armed Forces (MdA)[7] established a Cyber Defence Command, known as ComCyber, to coordinate military cyber operations.[8] France has had an offensive cyber doctrine since then.[9] The Strategic Review of Cyber Defence, in February 2018, represented another important turning point, with major institutional reforms announced in recognition of the gravity of the threat.[10] It clarified the organisation and integration of cyber operations among government entities, along with the national and international legal framework surrounding their use.[11] Drawing from airspace monitoring and defence, it established a standing cyber-security posture for a range of circumstances from peacetime to wartime.[12] It also marked a clear evolution away from the passive-defence model of 2008 to one of active defence, including through the development of offensive cyber capabilities, strategy and doctrine that focused on adversaries' military systems.

The departure point of the 2018 review was the fact that, despite considerable efforts, France considered that it was lagging behind the other four permanent members of the United Nations Security Council in terms of cyber defences.[13] The document stated that France would commit itself to analysing cyber threats with appropriate thoroughness and in sufficient detail.[14] It laid out new objectives for promoting stability in cyberspace, including through disincentives for those who might attack French targets. It included a new system of classification for cyber attacks, suggesting that the highest level would probably justify classification under the UN Charter as an unlawful use of force.[15] It identified three technologies essential to national cyber security: detection of attacks, encryption, and the radio and mobile-telephone network for use in a national emergency.[16]

In its very wide scope and urgent tone, the 2018 review stood out from most of the equivalent documents that other countries had published by then. Although it remains the case that France is broadly in line with the positions of the US and the United Kingdom – especially on whole-of-society coordination, national industrial imperatives and skills development – the review conveyed novel postures on a number of issues. Also of note, in September 2018 the MdA introduced a policy for the armed forces to counter disinformation.[17] This was followed by two further policies in 2019: the Ministerial Policy for Defensive Cyber Warfare[18] and Public Elements for the Military Doctrine for Offensive Cyber Warfare.[19] Presented as supporting the country's strategy of achieving cyberspace superiority, the policies foreshadowed the recruitment of 1,000 new cyber personnel and allocated €1.5 billion (US$1.8bn) to the armed forces up to 2025.[20]

In 2020 and 2021 the government announced new spending plans that reflected escalating concerns about cyber threats. The first of these provided a modest €136 million (US$161m), directed at better protection of government systems,[21] but in February 2021 the cash injection was €1bn (US$1.2bn), apparently over five years, accompanied by what was in effect a new cyber-security strategy.[22] Though published only as a 33-page press kit, it contains radical targets.[23] These are broadly in line with the overall themes of the 2018 Strategic Review of Cyber Defence but reveal a new urgency and a greater emphasis on sovereign capability and economic competitiveness in the ICT sector. In the cyber-security sector, one goal is to double the workforce from 37,000 to 75,000 over five years.[24]

France maintains a clear separation between defensive and offensive cyber operations. This means that ANSSI, the leading cyber-security agency, is dedicated exclusively to defensive operations and is not part of the intelligence community, unlike the National Security Agency (NSA) in the US or Government Communications Headquarters (GCHQ) in the UK. This distinction is important for some in France, based

on an assumption that the purposes and remit of an intelligence agency, not least its disposition towards secrecy, can interfere with some of the purposes and practices needed for civil-sector cyber security, including the need for greater transparency around cyber breaches.

Governance, command and control

The course France takes on cyber issues is set by the president, with the assistance of two bodies set up in 2018. Political decisions around the formulation of cyber-defence policy are the responsibility of the Defence and National Security Council (CDSN),[25] in which ANSSI is represented by the head of the SGDSN and ComCyber is represented by the Chief of the General Staff. Another body, the Cyber Defence Executive Committee, under the authority of the president, is tasked with high-level implementation of the decisions taken by the CDSN. The responsibility of the Cyber Defence Steering Committee, under the SGDSN, is to report once a year to the prime minister on the implementation of national cyber-security strategy.[26] In practice, meaningful decision-making on cyber security and defence begins in ministerial offices and extends up to the prime minister and the president.[27] The SGDSN then transmits the impetus of political leadership, sets the agenda and ensures the application of the measures decided.[28]

There are four channels of operational accountability: in the civil sector, through ANSSI to the prime minister; in the military, through ComCyber to the Chief of the General Staff; in the intelligence agencies, through the heads of agency to the relevant ministers; and for matters related to cyber crime, through the police, who work with prosecutors and judges.[29]

Below the head of ComCyber, each service remains responsible for its own defensive cyber operations and operates its own Security Operations Centre (SOC).[30] The Centre for the Analysis of Cyber Defence[31] is the MdA's SOC. It assesses global cyber risk so that ComCyber can then act and also advise the relevant government officials. The Centre for the Review of Information Systems Security[32] conducts penetration testing and security audits on military systems. The deployable branch of ComCyber is the 807th Signals Company, based in Rennes, whose mission in operations is to secure communications and weapons systems. ComCyber had 3,400 personnel in late 2019 and plans to reach 4,500 by 2025.[33]

As with other leading cyber powers, the efficiency of the command arrangements for French cyber operations is facilitated by high-quality technical systems, strong consensus within the relevant agencies, and political leadership that understands the value of cyber capabilities for a variety of missions.

Core cyber-intelligence capability

The focal point for the production of cyber intelligence in France is the General Directorate for External Security (DGSE).[34] But, as in the Five Eyes countries, all the French intelligence agencies have cyber capabilities and, in accordance with their specific areas of competence, cyber responsibilities. Other key agencies in the *premier cercle* of the intelligence community are the Defence Intelligence and Security Directorate,[35] the Directorate of Military Intelligence[36] and the General Directorate for Internal Security.[37]

In the cyber-security sector, one goal is to double the workforce from 37,000 to 75,000 over five years

Unlike in the Five Eyes countries, the French cyber model involves, at the national level, the strict institutional separation of offensive from defensive capabilities, and of core cyber intelligence from core cyber security. ComCyber, a military entity, takes the lead in offensive cyber operations, while cyber security is the responsibility of ANSSI. Another contrast with the Five Eyes countries is that the DGSE is an entity with overall national responsibility both for signals intelligence and for human intelligence collection. This means that the development of national cyber-intelligence capabilities is just part of the DGSE's remit: there is no French agency dedicated entirely to that role, in the way that the NSA is in the US or GCHQ in the UK. While this is just one of a number of factors that make direct comparisons problematic, the evidence suggests that France's annual investments

in core cyber-intelligence capabilities are markedly less than, for example, the UK's. Whether France's organisational integration of its human and technical capabilities and separation of cyber intelligence from cyber security have some practical advantages over the model used by its Five Eyes peers is a subject of much debate.

Overall, French cyber-intelligence capabilities seem strong on certain geographical regions, such as North Africa, but lack the global reach of the Five Eyes countries, in particular the US and the UK. Indeed, the French intelligence agencies were surprised by the sophistication of the Five Eyes capabilities revealed in the Snowden leaks. However, France's capabilities are amplified by international intelligence partnerships, including particularly close ones with some Western European states, including the UK, and with the US, as well as intelligence-sharing arrangements with some of its former colonies.

The French intelligence agencies were surprised by the sophistication of the Five Eyes capabilities revealed in the Snowden leaks

Another key contrast with the Five Eyes countries is the support that French intelligence services provide to French industry's involvement in extensive industrial espionage. One former director of the DGSE claims that, during his tenure, it devoted as much as a quarter of its resources to such activities.[38] Businesses, meanwhile, have an incentive to collaborate with the intelligence agencies because of the prospect of receiving intelligence in return. The cyber component has apparently become a key part of these industrial-espionage efforts, with targets reportedly including European multinational firms, Iranian organisations and several francophone African countries.[39]

Cyber empowerment and dependence

In terms of the digitisation of society and the economy, France is not one of the leaders among the world's developed countries. In 2020 it was ranked 15th out of the 28 members of the European Union (which still included the UK) in the EU's Digital Economy and Society Index,[40] while the ICT sector accounted for 4% of GDP,[41] comprised about 110,000 companies[42] and sustained more than 700,000 jobs.[43] In the digital economy more broadly, the banking sector is one of the strongest digital performers, with FinTech alone having created 120,000 jobs.[44] French companies are highly internationalised: web companies on average generate 39% of their turnover in international markets,[45] while 52% of FinTech start-ups operate in more than one country.[46] And France is also a major consumer of digital services: its companies spend more on information technology and cyber security than their counterparts elsewhere in Europe or in the US (and incur the lowest costs when cyber incidents occur).[47]

France's start-up and innovation environment, which has benefited from reforms initiated under President Macron, is dynamic and expanding. Station F in Paris, for example, is one of the largest start-up incubators in Europe and includes cyber-security projects supported by Thales Digital Factory and Microsoft. The main areas of expertise among cyber-security start-ups are artificial intelligence (AI), blockchain, privacy and secure collaborative tools. Almost 20% of them are ANSSI-accredited,[48] which not only certifies the reliability of their products and services but also allows them to supply the government.

France has considerable strengths in AI research and its commercialisation, ranking among the top five EU countries in that respect.[49] It ranked fifth in the world in terms of its contributions to the two most prestigious AI conferences in 2020.[50] The government announced an AI strategy in 2018, with key aims including the promotion of data-sharing between the private and public sectors; renewing the four strategic sectors of healthcare, the environment, transport, and defence and security; and establishing interdisciplinary AI research hubs with links to industry.[51] The government planned to provide funding of €1.5bn (US$1.75bn) over five years, until the end of 2022.[52]

France's internet infrastructure is becoming more resilient through the diversification of its points of presence, the increased capacity if its interconnections and its high number of international points of entry. It ranks fifth in Europe in terms of its number of interconnection points,[53] representing about 4% of the worldwide total.[54]

As for regional integration, Orange maintains a long-distance optical network (WELDON) connecting the 25 largest French cities to other European metropolitan centres such as Barcelona, Frankfurt, London and Madrid.[55] In terms of network sovereignty, it seems France's core networks rely mostly on US-made servers.[56] However, the industrial landscape seems sufficiently strong and diversified to offer avenues for a 'nationalisation' of France's core network if that were to become necessary: Thales, Atos-Bull and Orange are all Europe-leading or world-leading companies either in terms of mass or secure telecommunications. Legislation passed by the National Assembly in July 2019 means ISPs now need to obtain approval from the government before using foreign hardware.[57] As a result, the main French providers have turned their backs on Huawei. France is second only to the UK as a European landing point for transatlantic cables and is also a hub for those from Asia (through the Red Sea).

France has a policy of maintaining sovereign capabilities for its key military hardware (such as sensors, command and control, stealth technology and core networks). Thales is designing, manufacturing and deploying secure networks for the MdA and for the government as a whole.[58] The armed forces are increasingly relying on information and communications technology for their flagship platforms (next-generation frigates, and the *Rafale* F4 and *Scorpion* programmes) but hope to be able to operate successfully in environments with degraded communications, command and control.

France owns and maintains a wide range of military satellites for the purposes of secure communications, imagery and signals intelligence. It has taken a stronger stance on security aspects of outer space, which it now sees as a military domain in its own right, not merely the location of supporting infrastructure for terrestrial operations. It considers space situational awareness to be the first pillar of its strategic autonomy in space. The MdA is allocating €4.3bn (US$5.1bn) to the modernisation of all its satellites and radars, as well as to the passive and active protection of space assets.[59] In February 2021 the government announced the opening in Toulouse of a NATO Centre of Excellence for space research, intending to exploit what the government claims to be Europe's largest space ecosystem (home to France's Space Command, its Space Academy, leading international space companies, and related laboratories and research centres).[60]

Cyber security and resilience

France is in many respects the leading country in the EU for cyber-security and resilience planning. In 2020, for example, an authoritative report assessed that companies in France devoted a higher proportion of their IT spending to cyber-security measures than in any other EU country.[61] A study of cyber security in companies listed in the world's six leading stock-market indexes found the companies listed in Paris's CAC 40 to have the highest levels of maturity.[62] Nevertheless, in 2021 the government revealed its dissatisfaction with private- and public-sector responses to cyber-security threats by announcing an acceleration programme and appointing a national coordinator.[63] One of the most serious threats it identified was a fourfold increase in ransomware attacks during 2020, with local-government services among the most frequent targets.[64]

The branch of government in charge of coordinating the security of France's infrastructure is the SGDSN. Its responsibilities include implementing government policies on critical national infrastructure and choosing the companies responsible for operating it. The Defence Planning Law 2014–19 created regulatory obligations for those companies, whether public or private, in terms of the security of their networks and industrial-control systems, their threat-detection capabilities and their penetration testing. Government agencies are empowered under domestic law to audit and test the companies' cyber defences[65] and to undertake cyber operations to neutralise the source of attacks ('hack back').[66] In 2019 the government signed three-year agreements with eight leading manufacturing companies to improve their cyber security,[67] and the Financial Markets Authority published new regulations requiring digital-assets providers to have resilient information systems.[68]

In an attempt to improve public–private cooperation on cyber security, the government has announced the creation of a 'national cyber-security campus'. Its three main goals will be to double down on public awareness-raising and training; to foster the sharing of skills, tools

and data among cyber-security actors; and to build up domestic industrial capability for cyber security.[69] The head of project is the CEO of Orange Cybersecurity. ANSSI is also making progress on public–public cooperation, for example having signed partnerships with the financial, railway and civil-aviation authorities.[70] France's defensive capabilities are of a high standard. At the NATO *Locked Shields* exercise in 2019, the French team came first out of the 23 participating states.[71] In the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union, France was ranked third out of 175 countries.[72]

France's defence-procurement agency, the General Directorate for Armaments (DGA),[73] has a long-standing cyber-security department as part of its information-control (Maîtrise de l'information) branch. Tasked with protecting the information and weapons systems of the armed forces, it provides technical expertise in threat intelligence, upstream research and crisis support.[74] As part of its responsibilities it conducts vulnerability research on the armed forces' systems,[75] and since 2015 it has organised cyber war games.[76] In cyber defence, the DGA's research-and-development priorities are to produce highly resilient information systems, to find solutions that will ensure the security of weapons systems and to identify the best uses of AI in cyber operations (including offensive operations). A government-supported equity fund dedicated to defence investments, DefInvest, was set up in 2017 with an initial budget of €50m (US$59m) to support small and medium enterprises.[77]

France has established a unit within the SGDSN, the Committee against Information Manipulation,[78] to address the problem of politically motivated disinformation.[79] There have been at least two cases of significant cyber-enabled foreign interference: the hacking of TV5Monde in 2016 and the Macron Leaks in 2017. Specialists confidently attributed both incidents to Russia. Though a new law in 2018 established various mechanisms to prevent the spread of manipulated information during election campaigns, it remains to be seen how effective it will be. To raise awareness and promote good practices among allies, the MdA worked with the Atlantic Council in producing a 'post-mortem' analysis of the Macron Leaks.[80]

Global leadership in cyberspace affairs

On the international stage, France sees its responsibilities in the light of its status as one of the five permanent members of the UN Security Council and its leading positions in the EU and NATO. It seeks to maintain a form of inclusive multilateralism and to open up debates on cyberspace governance to non-state actors. Its 'International Digital Strategy' places great emphasis on promoting an 'open, diverse and trusted' cyberspace, in which it anticipates the EU can be a key player.[81] France aims to promote existing institutional mechanisms in order to 'limit hacking and destabilising activities' in cyberspace, notably through an international initiative, the 'Paris Call for Trust and Security in Cyberspace',[82] unveiled in November 2018. It is also actively involved in the related UN Group of Governmental Experts[83] and has been influential in the framing of the EU Cybersecurity Act. In 2019 France joined New Zealand in launching the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online, having earlier called for the creation of an appropriate regulatory framework within the EU.[84]

France pursues vigorous cyber diplomacy with key states on a bilateral level, as well as through mechanisms such as the G7. In 2020, for example, France and Germany published their third annual ICT security assessment.[85] In 2019 the third India–France cyber dialogue was held,[86] and France's presidency of the G7 saw the launch of an initiative on sharing best practices and lessons learned from the implementation of voluntary norms for cyberspace.[87] In 2018, in the Organisation for Economic Co-operation and Development, France initiated the annual Global Forum on Digital Security for Economic Prosperity, aimed at promoting the established French position that the private sector has a significant role to play in the security and stability of cyberspace.[88]

France has played a leading role in mobilising the EU's adoption of sanctions against the perpetrators of cyber attacks targeting European and national interests. In 2020 it joined the first EU sanctions against Russia and China in response to their cyber attacks,[89] which included a travel ban and asset freezes on four members of Russia's military intelligence directorate (GRU) and two Chinese nationals.[90] In its interpretation of international law,

France adopts a different position from its closest allies on the right to retaliate against cyber attacks below the threshold of armed attack, taking the view that it would be legitimate to retaliate against a series of attacks that together constitute hostile intent, even if, taken individually, none of them crosses the threshold.[91]

Offensive cyber capability

France's ComCyber has an operational complement of approximately 3,400 personnel (of which around 600 are reported to be ICT specialists), and aims to have 4,500 by 2025.[92] Its commander, General Didier Tisseyre, has stated that 40% of the personnel work on offensive operations, a share that is expected to grow in the coming years.[93]

Official and unofficial statements, as well as leaked forensic reports, have confirmed France's use of cyberspace for both disruption[94] and espionage.[95] According to General François Lecointre of the French Army, the country has also conducted cyber operations against terrorist groups in the Sahel and the Sahara.[96] Although there is little public evidence of France carrying out other destructive cyber operations, its record of robust retaliatory responses in national-security situations suggests it is prepared to do so in certain circumstances, as its leaders have acknowledged.[97] Official policy concerning offensive cyber operations places great emphasis on considering and mitigating political, legal and military risks of collateral damage to civilian infrastructure.[98] It is therefore unlikely that France would rely on private companies for offensive operations, beyond technical support.

Overall, we believe that France has a considerable offensive cyber capability. However, as in the closely related area of core cyber-intelligence capabilities, it probably lags behind the US and the UK.

Notes

1 Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2008, http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/livre_blanc_1337/livre_blanc_1340/index.html.

2 Agence nationale de la sécurité des systèmes d'information

3 Secrétariat général de la défense et de la sécurité nationale

4 Agence nationale de la sécurité des systèmes d'information, 'Défense et sécurité des systèmes d'information: Stratégie de la France', 2011, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

5 Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2013, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

6 Jean-Baptiste Jeangène Vilmer, 'The "#Macron Leaks" operation: A post-mortem', Atlantic Council, 20 June 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem.

7 Ministère des Armées

8 Ministère des Armées, 'Le commandement de la cyberdéfense (COMCYBER)', https://www.defense.gouv.fr/ema/organismes-interarmees/le-comcyber/le-comcyber/comcyber.

9 Ministère des Armées, 'Éléments publics de doctrine militaire de lutte informatique offensive', 2019, p. 4, https://www.defense.gouv.fr/fre/content/download/551497/9393997/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf. It was revealed in this 2019 document that an offensive cyber doctrine had been in place in 2017.

10 Secrétariat Général de la Défense et de la Sécurité Nationale, 'Revue stratégique de cyberdéfense', 12 February 2018, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

11 François Delerue and Aude Gery, 'France's Cyberdefense Strategic Review and International Law', Lawfare, 23 March 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

12 Arthur P. Laudrain, 'French Cyber Security and Defence: Strategy, Policy-Making and Coordination', SSRN Working Paper Series, v.2.3.3, 2019, p. 20, http://dx.doi.org/10.2139/ssrn.3432338.

13 Secrétariat Général de la Défense et de la Sécurité Nationale, 'Révue stratégique de cyberdéfense', p. 7.

14 *Ibid.*, p. 135.

15 *Ibid.*, p. 80.

16 *Ibid.*, pp. 96–100.

17 Florence Parly, 'Déclaration de Mme Florence Parly, ministre des armées, sur la manipulation de l'information', Vie publique, 4 September 2018, https://www.vie-publique.fr/discours/206652-declaration-de-mme-florence-parly-ministre-des-armees-sur-la-manipulat.

18 Ministère des Armées, 'Politique ministérielle de lutte informatique défensive', 2019.

19 Ministère des Armées, 'Éléments publics de doctrine militaire de lutte informatique offensive', 2019.

20 Ministère des Armées, 'Communiqué: La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive', 18 January 2018, https://www.defense.gouv.fr/fre/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive.

21 Agence nationale de la sécurité des systèmes d'information, 'Le Volet Cybersécurité de France Relance', September 2020, https://www.ssi.gouv.fr/agence/cybersecurite/le-volet-cybersecurite-de-france-relance.

22 'Un plan à 1 milliard d'euros pour renforcer la cybersécurité', Gouvernement.fr, 18 February 2021, https://www.gouvernement.fr/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite.

23 'Dossier de presse – Cybersécurité, faire face à la menace: la stratégie française', Gouvernement.fr, 18 February 2021, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/02/210218_dp_cyber_vfinale.pdf.

24 *Ibid.*, p. 6.

25 Conseil de defense et de sécurité nationale

26 Secrétariat Général de la Défense et de la Sécurité Nationale, 'Revue stratégique de cyberdéfense'.

27 Laudrain, 'French Cyber Security and Defence', p. 24.

28 *Ibid.*

29 This was recommended in the 'Revue stratégique de cyberdéfense', p. 53, and implemented by 2019. See Institut des hautes études du ministère de l'Intérieur, 'Organisation de l'État français en gestion de crise cybernétique majeure', 2019, https://inhesj.fr/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure.

30 Laudrain, 'French Cyber Security and Defence', p. 19.

31 Centre d'analyse de lutte informatique défensive

32 Centre d'audit de la sécurité des systèmes d'information

33 COMCYBER, 'GDA Tisseyre: "On est 3400 cybercombattants et on deviendra 4500 en 2025"', @ComcyberFR on Twitter, 12 September 2019, https://twitter.com/ComcyberFR/status/1172186486134968322.

34 Direction générale de la sécurité extérieure

35 Direction du Renseignement et de la Sécurité de la Défense

36 Direction du renseignement militaire

37 Direction générale de la sécurité intérieure

38 Isabelle Laumonier, 'Internet sous l'oeil des services de renseignement', Memoire Online, c. 2003, https://www.memoireonline.com/05/06/155/m_internet-sous-l-oeil-des-services-de-renseignement14.html.

39 'France and economic intelligence', Tarlogic, 6 November 2019, https://www.tarlogic.com/en/blog/france-and-economic-intelligence.

40 European Commission, 'EU Digital Economy and Society Index 2020', https://ec.europa.eu/digital-single-market/en/desi.

41 Eurostat, 'Percentage of the ICT Sector on GDP', https://ec.europa.eu/eurostat/web/products-datasets/-/tin00074.

42 Ministry of the Economy and Finance, 'Numérique: Chiffres clés', 14 March 2019, https://www.entreprises.gouv.fr/etudes-et-statistiques/numerique-chiffres-cles.

43 G. De Prato (ed.), *The 2018 PREDICT Key Facts Report: An Analysis of ICT R&D in the EU and Beyond*, European Commission, JRC Technical Report, 2018, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC112019/jrc112019_2018_predict_key_facts_report.pdf.

44 Ministry of the Economy and Finance, 'La Fintech, le numérique au service du secteur financier', 19 January 2018, https://www.economie.gouv.fr/entreprises/fintech-innovation-finance.

45 'La French Tech', Gouvernement.fr, https://lafrenchtech.com/en.

46 'Baromètre EY - FD', France Digitale blog, accessed 8 July 2019, http://www.francedigitale.org/barometre-ey-fd.

47 Hiscox, 'Hiscox Cyber Readiness Report 2019', https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF.

48 *Ibid.*

49 European Commission, Joint Research Centre, 'AI Watch: TES Analysis of AI Worldwide Ecosystem in 2009–2018', JRC Technical Reports, LU: European Commission, 2020, pp. 30–1, https://data.europa.eu/doi/10.2760/85212.

50 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216.

51 'AI for Humanity', AI for Humanity, 29 March 2018, https://www.aiforhumanity.fr.

52 *Ibid*.

53 Arcep, 'Baromètre de l'interconnexion de données en France', 27 June 2019, https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html.

54 Calculations based on data provided by Rowan Klöti et al., 'A Comparative Look into Public IXP Datasets', *ACM SIGCOMM Computer Communication Review*, vol. 46, no. 1, 11 January 2016, pp. 21–9, https://doi.org/10/f8bkst.

55 Orange, 'Les Réseaux d'Orange: dossier de presse', February 2019, https://www.orange.com/sirius/edossiers/pdfs/reseaux-orange-2017-fr/dp_reseaux_orange_fr_full.pdf.

56 France IX, 'France-IX's Infrastructure', https://www.franceix.net/en/technical/infrastructure.

57 Wei Shi, 'French parliament passes "Huawei Law" to govern 5G security', telecoms, 26 July 2019, https://telecoms.com/498728/french-parliament-passes-huawei-law-to-govern-5g-security.

58 'Thales Modernise Les Réseaux de Télécommunications Du Ministère de La Défense', Thales Group, accessed 9 July 2019, https://www.thalesgroup.com/fr/monde/press-release/thales-modernise-les-reseaux-de-telecommunications-du-ministere-de-la-defense; and 'Thales Assure La Sécurité de l'accès à Internet Du Réseau Interministériel de l'État', Thales Group, accessed 12 July 2019, https://www.thalesgroup.com/fr/worldwide/securite/press-release/thales-assure-la-securite-de-lacces-internet-du-reseau.

59 Arthur Laudrain, 'France's "Strategic Autonomy" Takes to Space', International Institute for Strategic Studies, Military Balance blog, 14 August 2019, https://www.iiss.org/blogs/military-balance/2019/08/france-space-strategy.

60 Ministère de l'Europe et des Affaires Étrangères, 'Defence – Establishment of the NATO space centre of excellence in Toulouse – Communiqué issued by the Ministry for the Armed Forces', 5 February 2021, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/article/defence-establishment-of-the-nato-space-centre-of-excellence-in-toulouse.

61 European Union Agency for Cybersecurity, 'NIS Investments Report', December 2020, p. 7, https://www.enisa.europa.eu/publications/nis-investments/at_download/fullReport.

62 Wavestone, 'Top Companies Cybersecurity Index: 2020 Annual Reports', https://www.wavestone.com/app/uploads/2020/07/Wavestone-Cyberindex-top-companies-2020-EN.pdf.

63 'Dossier de presse – Cybersécurité, faire face à la menace: la stratégie française', Gouvernement.fr, p. 12.

64 *Ibid*., pp. 7–11.

65 'Loi N° 2013-1168 Du 18 Décembre 2013 Relative à La Programmation Militaire Pour Les Années 2014 à 2019 et Portant Diverses Dispositions Concernant La Défense et La Sécurité Nationale – Article 22 | Legifrance', accessed 29 March 2019, https://www.legifrance.gouv.fr/eli/loi/2013/12/18/2013-1168/jo/article_22.

66 'Code de La Défense – Article L2321-2', L2321-2 Code de la défense § (2013).

67 G20 Research Group, '2019 G20 Osaka Summit Interim Compliance Report', p. 223, http://www.g20.utoronto.ca/compliance/2019osaka-interim/08-2019-g20-compliance-interim-cyber-resilience.pdf. The companies were Airbus, ArianeGroup, Dassault Aviation, MBDA, Naval Group, Nexter, Safran and Thales.

68 *Ibid*.

69 'Un campus cybersécurite pour renforcer l'écosystème français', Gouvernement.fr, accessed 25 July 2019, https://www.gouvernement.fr/partage/11104-un-campus-cybersecurite-pour-renforcer-l-ecosysteme-francais.

70 Agence nationale de la sécurité des systèmes d'information, 'Rapports d'activités', https://www.ssi.gouv.fr/agence/missions/rapports-dactivites.

71 'France Wins Cyber Defence Exercise Locked Shields 2019', NATO CCDCOE, 12 April 2019, https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019.

72 International Telecommunication Union, 'Global Cybersecurity Index 2018', pp. 30, 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

73 Direction générale de l'armement

74 Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2013.

75 Assemblée nationale, 'Rapport d'information de Mme Alexandra Valetta Ardisson et M. Bastien Lachaud Déposé En Application de l'article 145 Du Règlement, Par La Commission de La Défense Nationale et Des Forces Armées, En Conclusion Des Travaux d'une Mission d'information Sur La Cyberdéfense', 4 July 2018, http://www2.assemblee-nationale.fr/documents/notice/15/rap-info/i1141/#P439_94811.

76 'La DGA Développe Les Jeux de Cyberguerre à Bruz', IntelligenceOnline, 11 March 2015, https://www.intelligenceonline.fr/renseignement-d-etat/2015/03/11/la-dga-developpe-les-jeux-de-cyberguerre-a-bruz,108065256-bre.

77 BPI France, 'Definvest: Fonds d'investissement dédié aux entreprises stratégiques de la Défense', accessed 8 July 2019, https://

www.bpifrance.fr/Toutes-nos-solutions/Participation-au-capital/Fonds-d-investissement-thematiques/Definvest.

78 Comité de lutte contre la manipulation de l'information (CLMI)

79 Sénat, 'Délégation Parlementaire au Renseignement: Rapport d›activité 2019–2020', 11 June 2020, http://www.senat.fr/rap/r19-506/r19-50638.html.

80 Jeangène Vilmer, 'The "#Macron Leaks" operation: A post-mortem'.

81 Ministère de l'Europe et des Affaires Étrangères, 'Stratégie internationale de la France pour le numérique', Paris, 15 December 2017, https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-strategie-internationale-de-la-france-pour-le-numerique/#:~:text=Pr%C3%A9sent%C3%A9e%20par%20le%20ministre%20de,diplomatique%20des%20ann%C3%A9es%20%C3%A0%20venir.&text=Elle%20s'articule%20autour%20de,%3A%20gouvernance%2C%20%C3%A9conomie%2C%20s%C3%A9curit%C3%A9.

82 Arthur Laudrain, 'Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace', Lawfare, 4 December 2018, https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace.

83 Since a UN General Assembly resolution in 2004, a UN Group of Governmental Experts (GGE) has convened for two-year terms to address international-security aspects of cyberspace. It was known as the GGE on 'Developments in the Field of Information and Telecommunications in the Context of International Security' until 2018, when it was renamed the GGE on 'Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. In cyberspace-policy circles it is common to refer to it simply as 'the GGE'. See UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

84 Ministère de l'Europe et des Affaires Étrangères, 'Guaranteeing Cybersecurity', undated, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/article/guaranteeing-cybersecurity.

85 Federal Office for Information Security (Germany) and Agence Nationale de la Sécurité des Systèmes d'Information, 'Third edition of the Franco-German common situational picture', 2020, https://www.ssi.gouv.fr/uploads/2020/12/anssi-bsi-common_situational_picture_2020.pdf.

86 Ministère de l'Europe et des Affaires Étrangères, 'Indo-French Bilateral Cyber Dialogue', 20 June 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19.

87 Ministère de l'Europe et des Affaires Étrangères, 'G7 French presidency – Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices', 26 November 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/g7-french-presidency-cyber-norm-initiative-synthesis-of-lessons-learned-and.

88 Ministère de l'Europe et des Affaires Étrangères, 'Guaranteeing Cybersecurity', undated, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/article/guaranteeing-cybersecurity.

89 Ministère de l'Europe et des Affaires Étrangères, 'EU – Cyberattacks – Q&A from the press briefing', 30 July 2020, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20.

90 Lorie Maglana and Sunny Man, 'Europe: EU imposes the first ever sanctions against cyber-attacks', Global Compliance News, 21 August 2020, https://globalcompliancenews.com/eu-imposes-the-first-ever-sanctions-against-cyber-attacks-20200810.

91 Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 9 September 2019, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf.

92 Ministère des Armées, 'Le COMCYBER', 4 February 2021, https://www.defense.gouv.fr/ema/organismes-interarmees/le-comcyber/le-comcyber/comcyber.

93 Laurent Lagneau, 'Environ 40% des effectifs du Commandement de la cyberdéfense sont tournés vers les actions offensives', Zone Militaire, 9 May 2020, http://www.opex360.com/2020/05/09/environ-40-des-effectifs-du-commandement-de-la-cyberdefense-sont-tournes-vers-les-actions-offensives.

94 Nathalie Guibert, 'Général Lecointre: "L'indicateur de réussite n'est pas le nombre de djihadistes tués"', *Le Monde*, 13 July 2019, https://www.lemonde.fr/international/article/2019/07/12/general-lecointre-l-indicateur-de-reussite-n-est-pas-le-nombre-de-djihadistes-tues_5488379_3210.html.

95 Martin Untersinger and Jacques Follorou, 'La France suspectée de cyberespionnage', *Le Monde*, 21 March 2014, https://www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html.

96 Simon Pascal, 'Cyberdéfense. "Nous allons accroître encore les capacités de la plaque rennaise"', Ouest-France.fr, 18

December 2020, https://www.ouest-france.fr/politique/defense/cyberdefense-nous-allons-accroitre-encore-les-capacites-de-la-plaque-rennaise-7091506.

97 Robert S. Dewar (ed.), 'National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1', Center for Security Studies, 2018, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf.

98 Laudrain, 'French Cyber Security and Defence', p. 9.