FRANCE
CYBER READINESS AT A GLANCE

Principal Investigator: Melissa Hathaway
Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

September 2016

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

Acknowledgements

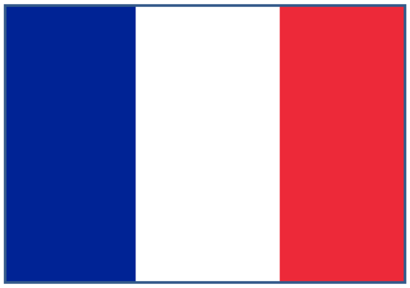
The Potomac Institute for Policy Studies and the authors would like to thank the following individuals for their contributions: Ms. Valérie Derouet-Mazoyer, Coordinator of the French Nuclear Industry Strategic Committee (CSFN) and Senior Vice-President, reporting to the EDF Group Senior Executive Vice-President in charge of nuclear generation; Ms. Frédérick Douzet (PhD), Chairwoman of the Castex Chair of Cyber Strategy and Professor at the French Institute of Geopolitics, Paris 8 University. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

FRANCE
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

FRANCE

CYBER READINESS AT A GLANCE



Country Population	66.6 million
Population Growth	0.5%
GDP at market prices (current $US)	$2.422 trillion
GDP Growth	1.2%
Year Internet Introduced	1981
National Cyber Security Strategy	2011, 2015
Internet Domain	.fr
Fixed broadband subscriptions per 100 users	40.2
Mobile broadband subscriptions per 100 users	66.2
Mobile phone subscriptions per 100 users	100.4

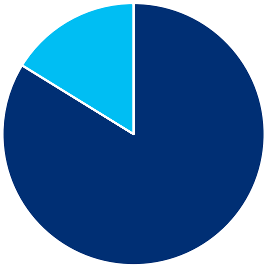
Information and Communications Technology (ICT) Development and Connectivity Standing

International Telecommunications Union (ITU) ICT Development Index (IDI)	**17**	World Economic Forum's Network Readiness Index (NRI)	**26**

Sources: World Bank (2015), ITU (2015), NRI (2015), and Internet Society.

INTRODUCTION

In 1981, a precursor to the Internet was first introduced in France via a video-text online service, called "Minitel," offered by the then state-owned France Telecom (or its predecessor Postes, Télégraphes et Téléphones, PTT) and only retired in 2012. While this service was text based, it was free to French citizens – as was the basic equipment; users could chat, make travel reservations and purchases, conduct online banking, and search telephone directories. This was both a technical and political project aimed at digitizing French society and ensuring France's technological independence.[1] The nationally sponsored program followed the guidelines of late 1940s French industrial policy, emphasizing national telecommunications investments as a key driver of economic advancement.[2] Minitel was eclipsed by the spread of the global Internet in the 1990s. Today, France is one of the most connected European countries with more than 83 percent Internet penetration – above the European Union (EU) average of 79 percent.[3] As of 2011, consistent with the 1940s French industrial policy goal, a quarter of French economic growth is now attributed to digital development.[4]



France Internet Penetration: 83.8%

With the release of the 2011 digital strategy, entitled "Plan France Numérique 2012-2020: Bilan et Perspectives," the French government redoubled its efforts to accelerate information communications technologies (ICTs) usage nationally – especially as a mechanism to generate employment and growth (unemployment rates hover around 11 percent for adults and around 25 percent for youth). In 2012, the French government launched the first EU project for a bond-funded venture for digital infrastructure to provide high-speed broadband (wireless) connection to French rural areas, with the aim to better distribute economic development throughout the country.[5]
In 2013, a national incentive plan was launched to distribute very-high-speed Internet to every household by 2025, using the best regionally adapted technology. Fixed broadband (by cable or telephone lines into a home or office) is now available across the entire country and growing rapidly.[6] Moreover, the ICT sector accounts for 3.7 percent of French jobs, 5.2 percent of gross domestic product (GDP), and 7.9 percent of total private-sector value added. Between 2014 and 2015, the ICT sector was expected to create more than 450,000 jobs and contribute €130 billion (~$146.6 billion) in value added.[7] The Plan France Numérique continues the French government's longstanding focus on telecommunications (now all ICTs) as a major means to build a competitive economy with full employment – especially for youth – and to reinforce French social values.[8]

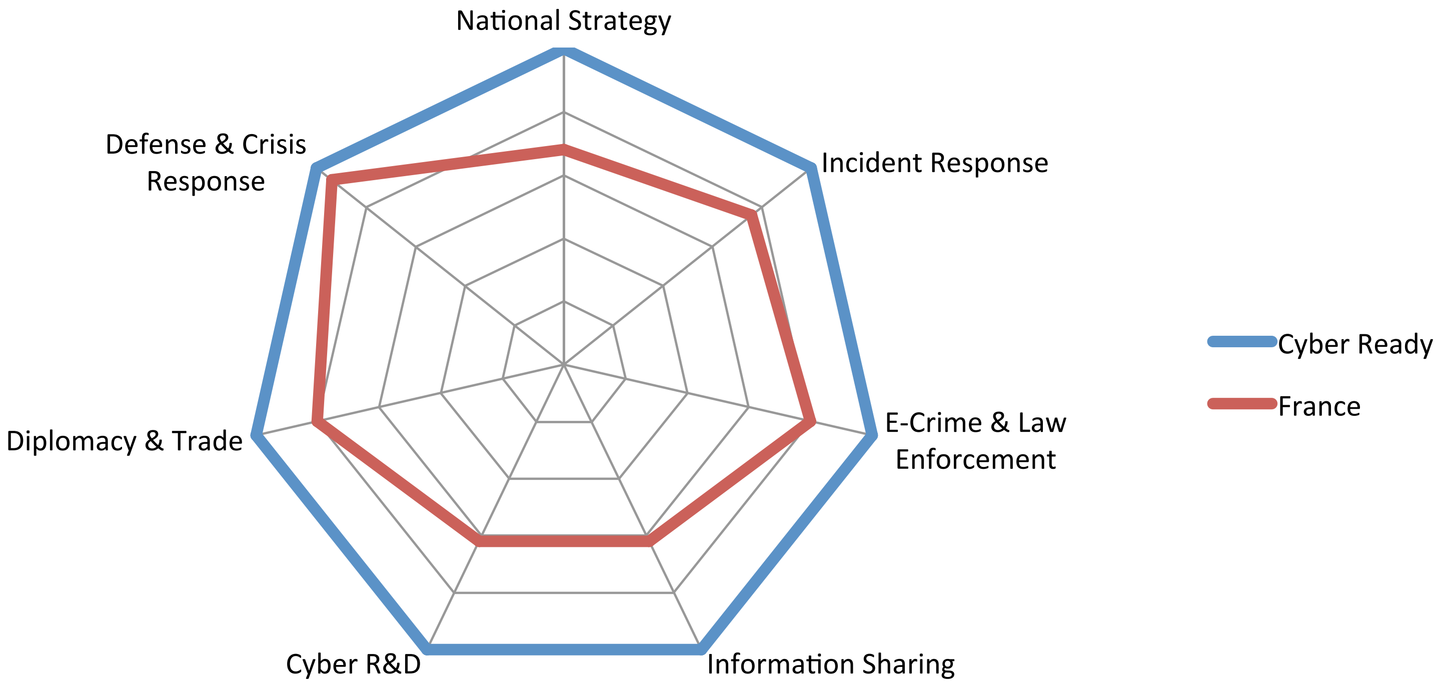
France's digital strategy set 57 targets to advance the French economy by 2020. Among those targets, the government seeks to: increase digital uptake to every company in France, convert all digital terrestrial channels to high-definition, and transition all government administration to paperless processes by 2020. In tandem with the digital strategy, France also launched a national ICT investment program, which includes the allocation of €2 billion (~$2.3 billion) for nation-wide Internet infrastructure (e.g., high speed mobile bandwidth, fiber optic, and digital transmission by satellite) by 2025; €2.25 billion (~$2.5 billion) to support innovative digital services, content, and applications; and €250 million (~$282 million) to develop smart grids. Furthermore, in 2012, the French government launched a "Greater Paris" project to make the capital city an advanced digital hub, attracting digital companies, talent, and investments internationally.[9] Lastly, the Public Investment Bank (BPI) recently launched an initiative called the "Digital Ambition Fund of BPI" to foster the development of digital start-up companies linked to the Internet and the emerging business models associated with the Internet of Things (IoT). Technology areas of interest include block-chain and cloud technologies, connected cars, digital marketing, security, and other digital products and services – with each area encouraging innovative business models. The BPI stated that it intends to make initial investments between €1million (~$1.1 million) and €10 million (~$11.2 million).[10]

Concurrent with these digital economic initiatives, France has also issued four high-level policy documents addressing how cyber insecurity is affecting French economy and security. In 2012, a French Senate report characterized the national cyber-related losses as a "systematic pillaging of its diplomatic, cultural, scientific, and economic inheritance."[11] The relevant set of central policy documents – which constitutes a comprehensive national cyber security strategy – are: (1) the 2008 "White Paper on National Defense and Security," (2) the 2011 "France's Cyber Strategy," (3) the 2013 "White Paper on National Defense and Security," and (4) the 2015 "French National Digital Security Strategy."[12] The latest document was announced by French Prime Minister Manuel Valls and was characterized as supporting the digital transition of French society. As Valls noted upon the release of the document, "by reinforcing digital security, we favor the development of a cyberspace that provides a sustainable source of growth and opportunities for French companies, thus asserting our democratic values and safeguarding our citizens' digital lives and personal data."[13]

The French government directly links its economic well-being to the cyber security of the nation. For example, three recent incidents highlighted how cyberspace can be used by terrorist groups to coordinate and plan attacks, then by news media to quickly inform the world about the attacks, and finally by national authorities to find the attackers. The satirical weekly newspaper *Charlie Hebdo* fell victim to a deadly shooting in January 2015 after it published content perceived to be irreverent to religious beliefs and current events. In November 2015, Paris fell victim to six armed attacks against different public locations including a night club and stadium. Investigations determined that the terrorists planned and coordinated the attacks using encrypted communications through WhatsApp and Telegram.[14] The latest July 2016 Bastille Day attack in Nice resulted in President Hollande's extension of the state of emergency that permits national security forces to engage in exceptional search-and-arrest operations and to monitor Internet use more freely.[15] Moreover, the French government has held a number of closed-door discussions with social media and search engine companies, and has asked them to work directly French authorities to immediately removing extremist propaganda when alerted by authorities.[16] In the interests of better assisting its citizenry, in June 2016, the French government launched a smart phone application intended originally to inform Euro 2016 fans of a potential terrorist attack; however, the government plans to use the application to build awareness of future risks.[17]

Cyber security was a recognized priority even before the 2015 and 2016 terrorist attacks. In 2001, the French government created, from its information security service, the Central Information Systems Security Division (DCSSI) under the authority of the General Secretary of National Defense to coordinate the cyber protection of the national government and infrastructure. In 2009, this central direction office evolved to become the French Network and Information Security Agency (Agence Nationale la Sécurité des Systèmes d'Information, ANSSI), which in 2011 published France's first national cyber security strategy. The same year, ANSSI became the national authority for information systems defense with whole-of-society responsibility, including providing guidance on protective measures – and sometimes regulations – for nationally significant industrial systems and corporations. Cyber security efforts are facilitated by the highly centralized role of the French government in both the economy and security of the country. The 2013 White Paper on National Defense and Security underlined that additional efforts were needed to achieve a secure cyberspace and stated that the development of offensive cyber capabilities was a necessary part of the French cyber defense strategy.[18] With the decision to create a cyber command immediately following the establishment of ANSSI, the French government signaled a whole-of-society approach towards mitigating cyber threats and aligning its economic vision with national security priorities.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate France's preparedness levels for cyber risks. This analysis provides an actionable blueprint for France to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment and maturity in closing the gap between its current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) is depicted in the Figure "France Cyber Readiness Assessment (2016)" on page 5.



France Cyber Readiness Assessment (2016)

1. NATIONAL STRATEGY

In recent years, France has conducted a profound overhaul of its defense and national security priorities to reflect the increase in scope, volume, intensity, and sophistication of national cyber threats, including cyber crime, political and economic espionage, attacks on critical infrastructure, and cyber disruption. The 2008 "White Paper on National Defense and Security" was the first major document to focus directly on the whole-of-the-nation cyber threats as a key risk to the country's security and sovereignty. It defined new priorities – such as cyber attack prevention and response – and ordered changes in the organizations charged with ensuring national security.[19] In line with the 2008 White Paper's recommendations, one of the three offices serving the Prime Minister directly – the office of the Secretary General for Defense of the Nation (Secrétariat Général

The Agency for National Network and Information System Security (ANSSI) was created in 2009 and serves as the national competent authority for the security of information systems.

de la Défense Nationale, SGDN) – was renamed the Secretary General for Defense and Security of the Nation (Secrétariat Général de la Défense et de la Sécurité Nationale, SGDSN). The change expanded the original mission from classic defense with armed forces to a wider responsibility for security of the whole society in circumstances beyond solely the use of armed forces or traditional national security agencies. This larger task was a reflection of the need to protect the society in more complex and turbulent times, especially given the rising challenge of cyber-enabled crime and state or non-state adversaries. In 2009, the Central Direction for Computer Security (DCSSI) became the Agency for National Network and Information System Security (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) and serves as the national competent authority for the security of information systems.[20] While focusing efforts to address the increasing challenge of cyber attacks on the country, ANSSI serves as an inter-ministerial organization of the Prime Minister's office, responsible for coordinating national cyber security effort across key industries and public agencies – including the military.[21] Since 2011, ANSSI has been formally designated as the national authority for the defense of information networks and systems in both public and private sectors.[22]

Following the creation of this agency, in 2011 France published its first national cyber security strategy, the "Information Systems Defense and Security: France's Strategy."[23] The 2011 strategy highlighted four major objectives: becoming a world leader in cyber defense, safeguarding France's decision-making ability through the protection of information related to sovereignty, strengthening the cyber security of critical infrastructure, and ensuring security in cyberspace. The 2013 "French White Paper on Defense and National Security" updated the previous 2008 version and specifically highlighted the threat of cyber sabotage against critical infrastructure.[24]

In 2015, the French government released its second national cyber security strategy – the "French National Digital Security Strategy" – in response to increasing volume of cyber

France published its 1st National Cyber Security Strategy in 2011 and released its 2nd iteration in 2015.

attacks of varying significance.[25] Building on previous security documents and the experience implementing the French digital strategy, the 2015 cyber security strategy aims to turn France into a "digital republic," recognizing that ICTs are both a catalyst of economic growth and innovation but are also imposing cyber risks.[26] The new strategy calls on the government to establish the means to protect France's fundamental interests in cyberspace, national information systems, and critical infrastructure. As a result, the French cyber security strategy lays out five key objective areas to drive France towards a "digital republic" while ensuring the security and resilience of French ICT systems. These five strategic priorities include: (1) defending French fundamental interests in cyberspace – such as state information systems and critical infrastructures; (2) ensuring digital trust, privacy, and the protection of personal data through the development of cyber security products and technical and legal assistance; (3) raising national cyber security awareness and capacity building; (4) developing a favorable and entrepreneurial environment for ICT investment and innovation for businesses; and (5) creating of a roadmap for European digital strategic autonomy.

France's 2015 cyber security strategy dovetails operationally with its 2011 digital strategy and many of the cyber security measures outlined in the digital strategy parallel the objectives in the cyber security strategy. For example, both documents seek to increase user trust online, maintain high levels of cyber security research and development as a driver of economic growth, and protect personal data. Most importantly, both documents recognize that ICTs underlie French economic growth, but also that ICT systems must be resilient and secure in order for France to fully reap the benefits of ICT-enabled growth. Although no new funds were included in the latest strategy, €1 billion (~$1.1 billion) was previously allocated for cyber security efforts. The release of the document by Prime Minister Valls signals the importance the French government is placing on cyber security.[27]

2. INCIDENT RESPONSE

In addition to serving as France's national competent authority for the security of information systems, ANSSI is also responsible for responding to cyber incidents "that affect the administrations and operators of vital importance," and for coordinating government, industry, and international incident response activities.[28] As the main entity in charge of cyber security in France, ANSSI acts as the government's Computer Emergency Response Team (CERT) by providing advice and recommendations with regards to the protection and integrity of public networks and critical infrastructure sectors, conducting audits of sensitive governmental information security infrastructure, and training government personnel. ANSSI regularly publishes on its website cyber security and best practices recommendations for government bodies, companies of all sizes, and the general public.

ANSSI also hosts the Operational Centre for the Security of Information Systems (Centre Opérationnel de la Sécurité des Systemes d'Information, COSSI), which is the government entity responsible for the detection and mitigation of cyber attacks directed at the state's information systems. In 2000, the French government established the first national CERT, located in COSSI and tasked with centralizing data and providing assistance in the event of cyber incidents.[29] Initially called "CERTA," the organization was renamed CERT-FR in 2014. As a part of ANSSI through COSSI, CERT-FR provides 24/7 incident handling services and acts as the main international point of contact for all cyber incidents affecting France, nationally. In particular, it provides in-depth analysis of identified vulnerabilities and malicious codes; monitors constituencies for cyber security incident; coordinates incident response measures for both government and entities engaged with critical infrastructure; provides alerts and information on incidents of national interest; and offers an email-based reporting structure to log cyber incidents.

France has a consolidated multi-domain national incident response plan called "Vigipirate" and one of the 12 domains is cyber security – covered by "Plan Piranet."[30] This plan aims to counter cyber attacks that would cause a major threat to the vital interests of the nation, people, property, environment, or vital activities of French organizations. This level of attack, as assessed by ANSSI, include: actions leading to widespread saturation or targeting of networks or systems (e.g., distributed denial of service); the widespread propagation of destructive software or precision targeting of the integrity of information systems (e.g., viruses, malicious software, ransomware, etc.); and broad based or specific denial, disruption, or destruction of information systems (e.g., takeover, sabotage, etc.).

In the 2013 "White Paper on Defense and National Security," France explicitly embraced a "proactive IT capacity associated with an intelligence capability" to expand the response options available to the government. This approach allows for actions involving "different stages, [that are] more or less reversible and more or less discreet, proportionate to the magnitude and seriousness of the attacks."[31] Echoing the 2008 White Paper, this later version reiterated that the capacity to detect and protect against cyber attacks and to defend sensitive information systems is "an essential component of [French's] national sovereignty" and economic well-being. Promising to increase the financial and human resources devoted to these tasks, the 2013 document asserted that the French government would define specific security standards, through legislative and regulatory procedures, for all operators of critical infrastructure (Opérateurs d'Importance Vitale, OIV) and sensitive systems in both the public

France established its first National Computer Emergency Response Team (CERT-FR) in 2000, tasked with centralizing data and providing assistance with incident response.

and private sectors. These imposed standards would particularly focus on audits, the mapping of enterprise information systems, handling and notification of incidents, and the capacity of ANSSI – and other state agencies when needed – to intervene in the event of a national crisis.

Furthermore, the Ministry of Defense is developing, in collaboration with ANSSI, a Reserve for Cyber Defense (RCD) force that will consist of 4,000 civilian reservists prepared to respond to a major crisis of the whole territory. In addition, a digital platform is planned to launch in 2017, providing assistance to cyber attack victims in public-private partnership for businesses and individuals.[32]

Since the French government has an overarching responsibility to ensure the security of critical infrastructure operators (OIVs), the 2013 French Military Planning Act (Loi de Programmation Militaire 2014-2019, LPM) also included four specific security measures that apply to government networks and private critical infrastructure operators.[33] As a result, ANSSI is authorized to (1) set mandatory security rules for critical systems of OIV, (2) mandate security inspections, (3) mandate specific measures in case of major crises, and (4) receive mandatory notification of incidents occurring on critical systems of OIV. Many of these actions anticipated the requirements of the new EU Network and Information Security (NIS) Directive adopted by the European Council in May 2016 and entered into force in August 2016.[34] France has already largely harmonized its domestic law to the new directive. Remaining actions include ensuring that French banks, telecommunication providers, and retailers implement intrusion detection systems as well as reporting any incident to ANSSI, which conducts audits on private and public entities subject to the law.

ANSSI, in cooperation with industry stakeholders, has also published additional proposals for sectors engaged with critical infrastructure, to help owners, operators, and government overseers better apply relevant cyber security rules. In addition, ANSSI and a group of private partners have launched a new accreditation initiative – the France "Cyber-security label" – for companies in the information technology (IT) and cyber security sectors. The aim of the accreditation process is to promote high standards of French security solutions for both domestic use and export to other markets.[35]

Finally, France conducts biennial national-level crisis management exercises organized by the SGDSN, including Piranet (dedicated to cyber) and other exercises such as: Pirate-Air, Pirate-Mer (sea), Pirate-Nuclear, Radilogical, Biolgical, Chemical (NRBC), and Metro-Pirate – each of them corresponds to a national-level plan and are protected and tightly held for national security reasons. The planning of these exercises can take up to six months and usually consists of a series of meetings between SGDSN, ministries, and private partners, during which the objectives, scenario, and injects for the exercises are discussed and formalized.[36] France participates also in multi-national exercises organized by the EU (e.g., Cyber Europe exercise) and by the North Atlantic Treaty Organization (NATO) (e.g., Locked Shields 2016).[37]

3. E-CRIME AND LAW ENFORCEMENT

In 2001, France signed and in 2006 ratified the Council of Europe Convention on Cybercrime (commonly known as the Budapest Convention). France is currently harmonizing its cyber security laws and is developing a series of new cyber crime laws. France is in favor of creating a system of simplified legal cooperation between EU member states to accelerate data sharing intended to curb cyber crime.[38]

The 2013 Military Planning Act followed the guidelines set by the 2013 "White Paper on Defense and National Security" calling for cyber security standards to help public and private sector operators of critical infrastructure protect themselves (with assistance from ANSSI) from cyber attacks.[39] After the 2015 *Charlie Hebdo* attacks, a new bill, the "Intelligence Bill," passed the French National Assembly allowing intelligence agencies to monitor phones, emails, and Internet usage of people suspected to have links to terrorism. The country has also strengthened existing regulations and laws allowing the government to shutdown websites deemed to be "sympathizing with terror." This new law now extends to surveillance of social media posts of suspected individuals as well.[40] However, major issues have surfaced with respect to the implementation of this requirement in terms of judicial investigation and content take-downs, leading to complex dynamics of conflict and cooperation with the platform providers.[41]

Moreover, the French government has updated the regulatory language of other cyber-related laws.[42] For example, in January 2016, the French National Assembly adopted a "Digital Republic" bill, enacting into law necessary measures supporting the framework of the 2011 national digital strategy.[43] It contained several new amendments to the French 1978 "Data Protection Act" – which had already been amended nine times with the latest version passed in 2014.[44] Most notably, it expanded the powers of the National Commission for Information Technologies and Liberties (Commission Nationale de l'Informatique et des Libertes, CNIL), including the ability to impose increased penalties for privacy violations including those associated with criminal activity.[45]

In 2014, the Ministry of Interior appointed a "cyber prefect" to coordinate MoI cyber activities and implement a ministerial action plan to fight cyber threats.

The police and the Gendarmerie in the Ministry of the Interior are responsible for fighting cyber crime. Since the late 1990s, the Gendarmerie – a military force charged with civilian police duties – has established multiple units to combat cyber crime including: a Cybercrime Department of Legal Research and Documentation (STRDJ), a Gendarmerie Criminal Research Institute (IRCGN), a Center for the Fight against Digital Crime (C3N), a National Center of Child Pornography Images (CNAIP), and specialized training programs in the National Center for Police Training (CNFPJ).[46] In addition, in 2014, the Ministry of the Interior (MoI) appointed a "cyber prefect" to coordinate MoI cyber initiatives and lead the implementation of a ministerial action plan to fight cyber crime and cyber economic espionage; thus building French resilience against cyber-related threats. The action plan has three strategic aims: to be more proactive in tackling cyber crime and supporting victims, to establish a more effective dialogue with cyber stakeholders, and to adopt related national and international legal frameworks.[47]

4. INFORMATION SHARING

As stated in the 2015 national cyber security strategy, France is committed to establishing domestic and international partnerships to promote the sharing of essential data (e.g., information on vulnerabilities or flaws of products and services) in order to ensure effective implementation of standards and appropriate security measures across all critical sectors. ANSSI is responsible for both incident response coordination and whole-of-society information sharing. Although the requirement to implement security standards on operators of critical infrastructure was legislated in 2013 with the Military Planning Act, it was not put into effect for three years. On 1 July 2016 it became effective, allowing ample time for ANSSI and the affected sectors to complete negotiations on how best to share information and implement standards to facilitate a stronger cyber defense posture.[48]

Moreover, the 2013 Military Planning Act requires OIVs to inform ANSSI about incidents that could endanger the functioning of respective IT systems. OIVs can be part of several sectors, including healthcare, utilities, telecommunication, transportation, and finance. In this context, several working groups have been set up per sector, in order to define efficient and compatible rules. In addition, the new 2016 "Digital Republic" law introduced three different provisions for expanded sharing of public sector information with citizens and other private entities, including – in principle – cyber security research of unclassified nature.[49]

While France has not established a dedicated government information sharing organization beyond the ANSSI, there are other mechanisms and information exchanges that are operational including non-profit research centers. For example, in 2014, a French National Anti-Botnet Support Centre – called Antibot.fr – was formed as part of a non-profit network of

The French National Anti-Botnet Support Centre assists the private sector with virus detection and clean up activities.

14 EU nations, that is funded by the European Commission under the ICT Policy Support Program for pilot programs. Jointly created by the French Expert Center Against Cybercrime (CECyF) and Signal Spam, the Center provides immediately useful information to prevent the spread of botnets. It also assists the private sector with cleaning up any associated viruses and with detecting infected websites and anomalies in networks.[50] Finally, there are at least 20 sector-specific CERTs in France that engage in information sharing activities consistent with their missions.[51]

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

France's 2011 digital strategy highlights the importance of investing in cyber security research and development (R&D) to promote economic growth. The strategy acknowledges the government's plan to invest €150 million (~$170 million) to support R&D in five strategic digital technologies and services: connected objects (Internet of Things), supercomputing, cloud computing, big data analytics, and the security of information networks.[52] As part of this strategy, the French government launched a "National Investment Programme," issuing an initial call for projects dedicated to R&D in cloud computing – which gained further support in the aftermath of the Snowden revelations.[53] Five projects received state aid amounting to €19 million (~$21 million) in investment: CloudForce by Orange, CloudPort by Prologue, Magellan by Bull, Nu@age by Non Stop System, and UnivCloud by INEO.

The digital strategy also includes support for small incubator programs. For example, the French government allocated €200 million (~$227 million) to Halle Freyssinet – an incubator site expected to accommodate more than 1,000 start-ups once operational in 2016.[54] France is also home to ICT innovation clusters, such as Cap Digital in the Ile-de-France, for the creation of digital content and its multimedia distribution and exchange; Images et Réseaux in Brittany and the Pays-de-la-Loire region, for communications networks; Secure Communication Solution in Provence, for secure processing and communications solution; and Systematic in the Ile-de-France, for complex systems and generic software.[55]

In October 2012, the French Government unveiled "The Greater Paris Project: Building a Digital City." The program is designed to set up world-class clusters for digital companies in Paris inner suburbs and surrounding areas in order to bring together players in the digital sector to stimulate momentum and encourage entrepreneurship and investment. Additionally, Fleur Pellerin – a former French Government Minister – launched "La French Tech" initiative, which labels dynamic cities with international profiles and a start-up culture as "Métropoles French Tech." The La French Tech initiative draws from the €200 million (~$223.4 million) investment fund aimed at turning France into a "digital republic" involving public and private sector actors.[56]

Additionally, the French government created various "Chairs of Research," funded by defense industrials in support of defense institutions such as the Castex Chair of Cyber

Strategy at the Institute of Higher National Defence Studies (IHEDN). The Institute brings together high-ranking managers from the civil service and the military for high-level training, reflection, and debate on strategic issues in defense, foreign policy, armaments, and defense economics. There are other research centers of excellence, including a Chair of Cyber Security at the special military school (École Spéciale Militaire) at Saint-Cyr focused on the Army, and a Naval Chair and Cyb'Air Chair focused on those respective military services' specific research areas.[57]

The development of France's cyber R&D industry is a key goal of the French government, which is aiming to turn the "Rennes region into a leading cyber hub in France and Europe."[58] The 2013 "White Paper on Defense and National Security" called for closer cooperation between government institutions – as well as industry – to combat cyber threats. In response, the French Ministry of Defense established a Cyber Defense Pole of Excellence (Pôle d'Excellence Cyber, PEC) in 2014. This center of excellence is co-located in Brittany with the Directorate General for Armaments for Information Security, which is responsible for integrating MoD's cyber skills in terms of training, research, and technology. The Rennes region is bringing together a tight network including the MoD's center of excellence, the Directorate General for Armaments, the MoD's Analysis Centre for Defensive Cyber Operations (Centre d'Analyse et de Lutte Informatique Defensive, CALID – which houses the MilCERT), the Army Signals General Staff, the 807th Cyber Defense Army Company, the School of Signals, the Special Military School of Saint-Cyr, as well as universities and cyber security businesses.[59]

The PEC is also intended to develop simulation and training capabilities available for the armed forces and employable in institutions outside the military.[60] For example, as of 2016, the PEC developed a Cyber West Challenge (CWC) contest for start-ups in the cyber sector, with a focus on cyber security and cyber defense. The CWC contest is supported by partners in the ICT sector, to include companies, banks, military units, and the University of Southern Brittany (Université de Bretagne-Sud). CWC prizes give specific support for start-ups in the cyber defense sector by offering a dedicated, secure space for their development in prox-

The French government is aiming to turn the Rennes region into a leading cyber hub in France and Europe.

imity to major contractors. The contest also plans to set up a cyber incubator, which would provide a favorable industrial, R&D, training and military ecosystem in an ideal geographic location.[61] Other cross-institution efforts are already underway involving universities, French industry, and government agencies.

Finally, in 2013, the French government launched a new reindustrialization plan called "The New Industrial France."[62] The second phase of the plan – "Industry of the Future" – rolled out in May 2015, and aims at preparing French industry for the digital age and includes plans across 34 industrial areas, several of which have a cyber component: smart grids, digital hospital, big data, cloud computing, e-education, augmented reality, contactless services, supercomputers, robotics, and cyber security. The French government has committed €3.7 billion ($4.1 billion) in new funding dedicated to this initiative.[63]

6. DIPLOMACY AND TRADE

The 2015 national cyber security strategy promotes "cooperation between member states of the European Union (EU) in a manner favorable to the emergence of a European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of our values."[64] In addition, the strategy reiterated the French government's intention to reinforce its "presence and influence in international discussions on cyber security… and to explore new regulatory mechanisms aimed at preventing conflicts in cyberspace … [and] consolidate[ing] a global base of commitments to good conduct in cyberspace for States, in compliance with international law."[65]

In line with the objectives described in the national cyber security strategy, France regularly participates in multilateral negotiations on cyber security and is a member of all major international bodies addressing cyber-related matters, most "notably the United Nations (UN) which acknowledged the application of international law to cyberspace in 2013."[66] France is considered a "key cyber power" within the UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which made the "affirmation that international law applies in cyberspace" the cornerstone of its 2013 report.[67] In 2015, the UN GGE agreed to a new report that proposed norms of responsible state behavior and included comments on the application of international law in cyberspace. The voluntary, non-binding norms contained in this report were ultimately adopted by the UN General Assembly in December 2015 and later endorsed by the G-20.

France actively contributes to the design of cyber security policy within other relevant international organizations including the Organisation of Economic Cooperation and Development's (OECD) Working Party on Information Security and Privacy (WPISP), which develops policy recommendations on the information society and resilience building.[68] France is also part of the Council of the EU's Friends of the Presidency [working] Group on cyber issues, launched in 2012. This group intends to provide a venue for EU member states to ensure horizontal coordination on cross-cutting cyber issues and exploit potential synergies among them.[69] In addition, France was deeply involved in the formation of the "Cybersecurity Strategy of the European Union" presented in February 2013 by the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy.[70]

Furthermore, France is an active member of the 2013 Wassenaar Arrangement on export controls, which aims to "enhance regional and international security and stability" by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. Through this agreement, France agreed to take on commitments "in respect of arms control [as] an integral part of its export policy which is subject to one of the most stringent national control procedures."[71] Most recently, France has been engaged in negotiations to finalize the Transatlantic Trade Investment Partnership (TTIP,) which includes several cyber elements. French officials, however, conceded that approval of this agreement in the near term is highly unlikely due to increased criticism in Europe, especially in France and Germany, that this deal "would serve as 'a breeding ground for populism' and be bad for Europe's economy."[72]

France has a stated policy of pursuing influence on the international stage by increasing investments in informal international fora that enhance collaboration among technical and academic communities and political decision-makers, and by promoting ICT exports and its cyber security industry internationally.[73] Unlike previous efforts characterized by isolated initiatives undertaken by different ministries, recent approaches have included more structured inter-ministerial coordination.

In 2014, the Ministry of Foreign Affairs and International Development established the role of Ambassador for Cyber Diplomacy and the Digital Economy.

The Ministry of Foreign Affairs and International Development serves as the office responsible for international cyber security engagement and the development of foreign policy that promotes a free, open, secure, and stable cyberspace. In October 2014, the Ministry created a specific cyber security coordinator position – the French Ambassador for Cyber Diplomacy and the Digital Economy – responsible for all international cyber security issues, including but not limited to agreement on standards for good governance, application of international law, protection of civil liberties and privacy, and promotion of French companies abroad.[74]

7. DEFENSE AND CRISIS RESPONSE

The French Ministry of Defense (MoD) is tasked with the protection of French national defense systems and providing aid to the nation as a whole, as requested.[75] The 2008 "White Paper on Defense and National Security" highlighted cyber security as a key national security priority and made recommendations for development of "both offensive and defensive cyber-war capabilities."[76] Before the measures detailed in the White Paper could be fully implemented, however, the Conficker worm had already infected many of the unclassified French military intranets. This infection caused messaging and logistic perturbation between services that impacted operations. Fighter aircraft missions were only moderately impacted as alternate means of exchange were available and the classified operational networks were not impacted.[77]

The equivalent of a French "cyber command" has emerged under the Cyber Defense General Officer along with the related staff, missions, and capabilities.

Since that time, the MoD has been vigorously engaged in a transformation process to professionalize, reorient strategically, and – in particular – actively prevent and mitigate potential cyber challenges to national defense and military networks. In 2009, the French government created ANSSI as a new step in a process that also involved the nation's armed forces and related intelligence institutions across armed and police forces. In the 2011 national cyber security strategy – the "Information Systems Defence and Security: France's Strategy" – the French government declared an intent to become a "world power in cyber defence," and strengthened the authorities of ANSSI.[78] In the same year, in its 2011 Joint Doctrine for Cyber, the French MoD established a Cyber Defense General Officer (labeled the "OG Cyber") position and associated units, such as the Cyber Defense Operational Command located within the Joint Operations Planning and Command & Control Centre (Centre de Planification et de Conduite des Opérations, CPCO).[79] The Cyber Defense General Officer is charged with guaranteeing the MoD's information system protection in the event of a crisis and collaborates closely with ANSSI to protect the rest of the nation as required.[80]

The 2013 "White Paper on National Defense and Security" followed the 2008 White Paper in further elevating the criticality of the MoD in order to provide a full spectrum of cyber defense capacities for the nation.[81] In the document, France recognizes that "cyberspace has thus become an area of confrontation," and notes that a cyber attack "could easily paralyze whole swathes of a country's activity, trigger technological or ecological disasters and claim numerous victims. It could therefore constitute a genuine act of war."[82] Furthermore, in this document, the MoD identifies a need for both advanced "identification and offensive action capabilities," labeling them "essential to implementing a possible and appropriate response to such attacks."[83] The document affirmed also that "the Ministry of Defense must continue to operate in all circumstances even – and above all – when many other organizations see their functioning damaged or obstructed by cyber attacks."[84]

To implement the ambitious goals related to cyber defense stated by the 2013 White Paper, in 2014, the MoD announced a €1 billion (~$1.1 billion) Cyber Defense Pact ("Pacte Défense Cyber 2014-2016"). The document had six major goals: (1) heightening the level of security of the defense ministry's information systems as well as those of trusted partners, (2) preparing for the future by intensifying research efforts in the technical, academic and operational fields while supporting the industrial base, (3) strengthening human resources attached to cyber defense, (4) developing a Cyber Defense Pole of Excellence in Brittany for the MoD and the cyber defense community, (5) cultivating a network of foreign partners in Europe and in areas of strategic interest, and (6) furthering the emergence of a national cyber defense community based on a circle or partners and the reserve networks.[85] The document listed fifty measures to set out a national cyber defense doctrine and achieve overarching and ambitious goals. These measures included the strengthening of the organizations established in 2011, reinforcing the command authorities of the OG Cyber, and further operationalizing the units available for both defense and – to a lesser extent – offense.[86] The improvements involved greater collaboration with ANSSI to prepare for emergencies, including co-locating the MoD's Analysis Centre for Defensive Cyber Operations (Centre d'Analyse et de Lutte Informatique Defensive, CALID – which houses the MilCERT) in the same premises.[87] The CALID "is the central expertise repository for the Department of Defense and serves as the readiness and reaction center for computer attacks (MilCERT) of the Department of Defense; which carries out surveillance and detection missions 24/7, seeking cyber attacks targeting the armies."[88] In addition, the 2014 Cyber Defense Pact called for the development of a national operational cyber defense reserve (Réserve de Cyber Défense, RCD), intended to assist the nation and the MoD in the event of a major crisis. These reserve units are to be developed in close cooperation with ANSSI and the Gendarmerie Nationale.[89]

Taken together, the equivalent of a "cyber command" has emerged under the OG Cyber along with the related staff, missions, and capabilities.[90] More precisely, this senior officer sits at the top of the operational command chain for cyber security and defense under the French Chief of Defense. The OG Cyber "has an operational role in the Planning and Operations Centre, [where] he is responsible for the planning, coordination, and conduct of cyber defence with regard to the MoD's and armed forces' information systems and of cyber operations in support of military operations." He is also "in charge of coordinating and developing cyber defence across the MoD as well as in the three services."[91] Thus, he commands cyber units as well as conducts preparations and planning within the French Joint Staff Cyber Defense Section dedicated to cyber operations. A key staff officer – the Central Computer Warfare Officer (Officier de Lutte Informatique Defensive, OLID) – oversees the deployment of the cyber forces within the armed forces, while a cyber management team implements the OG Cyber's decisions.[92]

The cyber portion of the defense budget has been increased in parallel with the enlargement of missions and units. In 2014, the Defense Minister announced the allocation of over €1 billion ($1.1 billion) towards the fifty measures listed in the Cyber Defense Pact 2014-2016.[93] For example, some of the funds were intended to double the personnel at the Cyber Defense Center of Excellence in Brittany from about 250 to 450. Overall, the French government has met the North American Treaty Organization's (NATO) minimum GDP defense spending requirement for of 2 percent – spending 2.1 percent of its GDP on defense in 2015 – of which an increasing proportion is dedicated to cyber-related activities.[94]

In general, the French armed forces are an active participant in domestic and allied cyber exercises – as noted in the incident response section – and especially in all those associated with NATO cyber defense exercises such as "Cyber Coalition." In the 2014 Cyber Defense Pact, the MoD stated a goal to "systematically include a cyber defence aspect at every level of armed forces exercises."[95] The exercises are intended to serve as a way to ensure the capacity of the armed forces to operate at every echelon during cyber attacks, disruptions, or credible threat postures, including the "ability to include cyberspace in their maneuver space" routinely.[96] In 2015, France held the first ever Cyber Defense International Forum with 26 foreign delegations in attendance, which focused on a variety of international cyber issues.[97]

Finally, the French MoD is an active player in the nation's domestic cyber defenses during crises. For example, in response to the 2015 *Charlie Hebdo* attack and a subsequent surge of cyber attacks against civilian and military targets, the French General Staff of the Armed Forces activated a cyber crisis cell for the first time in France's history.[98] After the 2016 Bastille Day attack in Nice, the French MoD called up at least 12,000 reservists, some of whom were part of the cyber defense reserve forces.[99]

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, France is on a path to becoming cyber ready, and is currently partially operational in all of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As France continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path towards a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

Legend

● **Fully Operational**

◐ **Partially Operational**

○ **Insufficient Evidence**

IDI Rank			NRI Rank	GDP Rank	National Strategy	Incident Response	E-Crime & Law Enforcement	Information Sharing	Investment in R&D	Diplomacy & Trade	Defense & Crisis Response
17	France	🇫🇷	26	6	◑	◑	◑	◑	◑	◑	◑

ENDNOTES

1. Hugh Schofield, “Minitel: The Rise and Fall of the France-wide Web,” *BBC News*, June 28, 2012, http://www.bbc.com/news/magazine-18610692.

2. James Foreman-Peck, “European Industrial Policies in the Post-war Boom: ‘Planning the Economic Miracle’,” in *Industrial Policy in Europe After 1945*, ed. Christian Grebas and Alexander Nützenadel (London: Palgrave Macmillan, 2014): 14, http://www.palgraveconnect.com/pc/doifinder/view/10.1057/9781137329905.0008.

3. World Bank, “Internet Users (per 100 People),” 2014, http://data.worldbank.org/indicator/IT.NET.USER.P2.

4. Premier Ministre, “France numérique 2012-2020: Bilan et perspectives,” November 2011, http://www.entreprises.gouv.fr/files/files/directions_services/secteurs-professionnels/etudes/2011_plan_france_numerique2020.pdf.

5. Cécile Barbière, “France Launches EU’s First Digital Infrastructure ‘Project Bond’,” *EuroActiv*, October 15, 2015, http://www.euractiv.com/section/regional-policy/news/france-launches-eu-s-first-digital-infrastructure-project-bond/.

6. Pascal Brangetto, “National Cyber Security Organisation: France,” *NATO Cooperative Cyber Defense Center of Excellence* (2015): 5.

7. Embassy of France in London, “France Aims to Put Tech at the Heart of its Economy by 2020,” *France in the United Kingdom*, http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

8. OECD, “OECD Digital Economy Outlook 2015,” (OECD Publishing: Paris): 21, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

9. Embassy of France in London, “France aims to Put Tech at the Heart of its Economy by 2020.”

10. BPI France, “Le Fonds Amibition Numérique,” December 2, 2011, http://www.bpifrance.fr/Bpifrance/Nos-metiers/Fonds-propres/Fonds-directs-Bpifrance/Capital-Innovation/Le-Fonds-Ambition-Numerique.

11. French Senate, “Rapport Bockel,” July 18, 2012, http://www.senat.fr/notice-rapport/2011/r11-681-notice.html.

12. Premier Ministre, “French National Digital Security Strategy,” (2015), http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

13. ANSSI, “Cybersecurity in France,” http://www.ssi.gouv.fr/en/cybersecurity-in-france/.

14. “2015 Paris Terror Attacks Fast Facts,” *CNN*, April 13, 2016, http://www.cnn.com/2015/12/08/europe/2015-paris-terror-attacks-fast-facts/.

15. Matthew Dalton and Sam Schechner, “France Tried to Ramp Up Defenses Ahead of Paris Attacks,” *The Wall Street Journal*, November 14, 2015, http://www.wsj.com/articles/paris-attacks-underscore-security-challenge-1447462066.

16. “France Asks US Internet Giants to ‘Help Fight Terror’,” *Al Jazeera*, February 21, 2015, http://www.aljazeera.com/news/2015/02/france-asks-internet-giants-fight-terror-150221063706705.html.

17. “France Launches a Terrorism App,” *Security Magazine*, June 9, 2016, http://www.securitymagazine.com/articles/87182-france-launches-a-terrorism-app.

18. Ministry of Defense, “French White Paper on Defence and National Security,” (2013): 43, http://www.ladocumentationfrancaise.fr/rapports-publics/134000257-livre-blanc-sur-la-defense-et-la-securite-nationale-2013?xtor=EPR-526.

19. Ministry of Defense, “The French White Paper on Defence and National Security,” (2008): 12.

20. ANSSI, “Cybersecurity in France.”

21. Pascal Brangetto, “National Cyber Security Organisation: France,” *NATO Cooperative Cyber Defense Center of Excellence* (2015): 9

22. NATO Parliamentary Assembly: Science and Technology Committee, “Cyber Space and Euro-Atlantic Security,” *Special Report*, (November 2014): 9.

23. Premier Ministre, “Information Systems Defence and Security: France’s Strategy,”(2011), http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

24. Ministry of Defense, “French White Paper on Defence and National Security,” (2013).

25. Premier Ministre, “French National Digital Security Strategy,” (2015).

26. *Ibid*, 3.

27. Tom Reeve, “French Government Launches National Cyber Security Strategy,” *SC Magazine*, October 19, 2015, http://www.scmagazineuk.com/french-government-launches-national-cyber-security-strategy/article/447973/.

28. Premier Ministre, “French National Digital Security Strategy,” (2015): 20.

29. ANSSI, “CERT-FR – Centre gouvernemental de veille, d’alerte et de réponse aux attaques informatiques,” http://www.cert.ssi.gouv.fr/.

30. ANSSI, “Plan Piranet,” http://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/.

31. Ministry of Defense, “French White Paper on Defence and National Security,” (2013).

32. Melissa Hathaway's interview with Valérie Derouet-Mazoyer, Coordinator of the French Nuclear Industry Strategic Committee (CSFN), September 16, 2016.

33. Legifrance, "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," https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825.

34. European Council, "EU-wide Cybersecurity Rules Adopted by the Council," May 17, 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/.

35. "Cyber-security: France Leads the Way in Europe," *Media Econocom Blog*, May 7, 2015, http://blog.econocom.com/en/blog/cyber-security-france-leads-the-way-in-europe/.

36. ANSSI, "French Cybersecurity Exercises," June 27, 2012, https://www.enisa.europa.eu/events/cyber-exercise-conference/presentations/9.%20Conf%20Paris%20-June%202012-%20-%20A.%20OGEE%20-ANSSI%20France.pdf, and ANSSI, "Cyber-attaques: l'exercice PIRANET 2012 met l'État à l'épreuve d'une crise informatique majeure," http://www.ssi.gouv.fr/publication/cyber-attaques-lexercice-piranet-2012-met-l-etat-a-lepreuve-dune-crise-informatique-majeure/.

37. Thomas Renard, "The Rise of Cyber Diplomacy: the EU, its Strategic Partners, and Cyber-Security," *European Strategic Partnerships Observatory* 7 (June 2014): 14, http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

38. Government of France, "French National Digital Security Strategy," (2015): 23.

39. Legifrance, "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," https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825.

40. Alessandria Masi, "France's Online War on Terror Sympathizers and Extremists has a New Cyber Security Cell," *IBT*, http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-security-cell-1786662.

41. Melissa Hathaway's interview with Professeure Frédérick Douzet (PhD), Chairwoman of the Castex Chair of Cyber Strategy and Professor at the French Institute of Geopolitics, Paris 8 University, September 8, 2016.

42. Premier Ministre, "French National Digital Security Strategy," (2015): 15.

43. Government of France, "Explanatory Memorandum," January 2016, http://www.republique-numerique.fr/pages/digital-republic-bill-rationale.

44. Commission Nationale de l'Informatique et des Liberties, "Loi Informatique et Libertes, Act No. 78-17 January 1978 on Information Technology, Data Files and Civil Liberties," (January 1978), https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

45. Nadège Martin and Geoffroy Coulouvrat, "French National Assembly Adopts "Digital Republic" Bill," *Norton Rose Fulbright*, March 10, 2016, http://www.dataprotectionreport.com/2016/03/french-national-assembly-adopts-digital-republic-bill/.

46. Gendarmerie Nationale, "Cybercriminalité," http://www.gendarmerie.interieur.gouv.fr/Notre-Institution/Nos-missions/Police-judiciaire/Cybercriminalite.

47. Government of France, "Cybersecurity: the Government's Strategy," January 28, 2016, http://www.gouvernement.fr/en/cybersecurity-the-government-s-strategy.

48. Reynald Fléchaux, "Cybersécurité: les grandes entreprises trouvent un modus vivendi avec l'Assi," *Silicon*, January 26, 2016, http://www.silicon.fr/cybersecurite-grandes-entreprises-trouvent-modus-vivendi-anssi-136930.html.

49. Samuel Greengard, "France Embraces Digital Transformation," *Communications of the ACM*, June 3, 2016, http://cacm.acm.org/news/203101-france-embraces-digital-transformation/fulltext.

50. Antibot, "Lancement d'Antibot.fr," December 10, 2014, http://www.antibot.fr/blog/lancement-d-antibot.fr.

51. ANSSI, "Les CSIRT Français," http://www.cert.ssi.gouv.fr/cert-fr/cert.html.

52. OECD, "OECD Digital Economy Outlook 2015," (OECD Publishing: Paris): 24.

53. Melissa Hathaway's interview with Professeure Frédérick Douzet (PhD),September 8, 2016.

54. *Ibid*.

55. Embassy of France in London, "France Aims to Put Tech at the Heart of its Economy by 2020," France in the United Kingdom, http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

56. *Ibid*.

57. Melissa Hathaway's interview with Professeure Frédérick Douzet (PhD), September 8, 2016.

58. Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," *Information & Security: An International Journal*, vol. 32 (2015): 9, http://connections-qj.org/system/files/3209_france.pdf.

59. *Ibid*.

60. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 16.

61. "Cyber West Challenge," http://www.cyberwestchallenge.bzh/en/.

62. Embassy of France in London, "The Industry of the Future," September 17, 2015, http://www.ambafrance-uk.org/The-Industry-of-the-Future.

63. Trade Bridge Consultants, "President François Hollande Launches 'New Industrial France'," http://tradebridge-consultants.com/news/government/president-francois-hollande-launches-new-industrial-france/.

64. Premier Ministre, "French National Digital Security Strategy," (2015): 9.

65. *Ibid*, 39-40.

66. *Ibid*, 8.

67. CCDCOE, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

68. Thomas Renard, "The Rise of Cyber-Diplomacy: the EU, its Strategic Partners and Cyber-Security," *European Strategic Partnership Observatory*, (June 2014):12, http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

69. *Ibid*, 13.

70. Ministry of Foreign Affairs, "France and Cyber Security," December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

71. "French Policy on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," http://www.wassenaar.org/wp-content/uploads/2015/12/fr1_en.pdf.

72. AFP, "EU-US Trade Deal 'Impossible' in 2016: French Minister Matthias Fekl," *The Economic Times*, July 5, 2016, http://economictimes.indiatimes.com/news/international/business/eu-us-trade-deal-impossible-in-2016-french-minister-matthias-fekl/articleshow/53065263.cms.

73. Premier Ministre, "French National Digital Security Strategy," (2015): 40.

74. Ministry of Foreign Affairs, "France and Cyber Security," December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

75. Pascal Brangetto, "National Cyber Security Organisation: France," *NATO Cooperative Cyber Defense Center of Excellence* (2015): 11.

76. Ministry of Defense, "The French White Paper on Defence and National Security," (2008): 9.

77. Kim Willsher, "French Fighter Plans Grounded by Computer Virus," *The Telegraph*, February 7, 2009, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

78. Premier Ministre, "Information Systems Defence and Security: France's Strategy," *ANSSI*, (2011), http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

79. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 5.

80. Ministry of Foreign Affairs, "France and Cyber Security."

81. "Europe Proposes New Laws and Regulations on Cybersecurity," *Jones Day*, January 2014, http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014/.

82. Ministry of Defense, "French White Paper on Defence and National Security," (2013): 4, 43.

83. *Ibid*, 7.

84. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 5.

85. Ministry of Defense, "Présentation du Pacte Défense Cyber," November 2, 2014, http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber.

86. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 6-9.

87. NATO Parliamentary Assembly: Science and Technology Committee "Cyber Space and Euro-Atlantic Security," *Special Report* (November 2014): 9.

88. Michel Baud, "American Military Cyberdefense, An Example for France?," *Chaire de CyberDéfense et Cybersecurité*, Saint-Cyr Publication Series, vol. 111, n. 8, (July 2013): 1-3.

89. Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," (2015): 9.

90. CyberDef-CyberSec, "4th Cyber Def – Cyber Sec Conference 2016," June 14, 2016, Paris.

91. Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," (2015): 8.

92. Michel Baud, "American Military Cyberdefense, an Example for France?," 3.

93. Ministry of Defense, "Cyberdéfense," *Direction Général des Relations Internationales et de la Stratégie*, June 22, 2016, http://www.defense.gouv.fr/dgris/enjeux-transverses/.cyberdefense/cyberdefense.

94. Pascal Brangetto, "National Cyber Security Organisation: France," (2015): 12.

95. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 9.

96. *Ibid*, 9.

97. Melissa Hathaway's interview with Professeure Frédérick Douzet (PhD), September 8, 2016.

98. Nathalie Guibert, "Cyberattaques: l'armée a activé pour la première fois une cellule de crise," *Le Monde*, January 1, 2015, http://www.lemonde.fr/pixels/article/2015/01/17/cyberattaques-l-armee-a-active-pour-la-premiere-fois-une-cellule-de-crise_4558160_4408996.html?xtmc=cyber&xtcr=1.

99. "Nice Attack: France Calls up to 12,000 Reservists," *BBCNews*, July 17, 2016, http://www.bbc.com/news/world-europe-36817435.

For more information or to provide data to the CRI 2.0 methodology, please contact:
CyberReadinessIndex2.0@potomacinstitute.org

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. She serves as a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies and is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barak Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html.

Chris Demchak is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. Her research areas are digital resilience, cyber conflict, and the structures and risks of cyber space. She designed a digitized organization model known as "Atrium" that helps large enterprises respond to and accommodate surprises in their systems. She is also the author of *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security*.

Jason Kerben is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. He also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security. In particular, he focuses on legal and regulatory regimes that impact an organization's mission. He develops methodologies and approaches to assess and manage cyber security risk and advises on a myriad of specific cybersecurity activities including international principles governing information and communications technologies, identity and access management, continuous diagnostics and mitigation and cyber insurance.

Jennifer McArdle is a Non-Resident Fellow at the Potomac Institute for Policy Studies and an Assistant Professor of Cybersecurity at Salve Regina University in Newport, RI. Jennifer's academic research and publications focus on cyber conflict, escalation management, and military innovation. She is a PhD candidate in War Studies at King's College London.

Francesca Spidalieri is a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. She also published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org