Information & Security: An International Journal

Vitel & Bliddal, vol.32, 2015 http://dx.doi.org/10.11610/isij.3209

FRENCH CYBER SECURITY AND DEFENCE: AN OVERVIEW

Philippe VITEL and Henrik BLIDDAL

Abstract: As threats to and in cyber space as well as the threats enabled by cyber space have burgeoned, cybersecurity and defence has emerged as a key policy area for governments around the world. For a long time, France has lagged behind its main strategic partners in these areas. However, in the recent years, the country has undertaken considerable efforts to catch up, leading to conceptual reformulation, organisational reforms, and substantial increases in resources. This article provides an overview of the conceptual basis for French cybersecurity and defence policies, the most important elements of its organisational set-up, and recent cyber efforts and initiatives. The article does not claim to be exhaustive, but aims to provide a starting point for structuring related research. While many French ministries and agencies are involved in cybersecurity, this article focuses on the efforts of the National Information Systems Security Agency (L'Agence nationale de la sécurité des systèmes d'information, ANSSI) and the ministries of defence and interior – the actors most heavily involved in French cybersecurity and defence.

Keywords: Cybersecurity; cyber defence; French defence and security policies; organisation of national security and defence; cyber terrorism; cyber war, ANSSI.

Introduction

We live in an information society and in a "cyber" era, premised on the widespread use of connected information technologies and telecommunications, most notably the Internet. Over the last quarter-century, cyber space has become a fundamental pillar of modern life – to the degree that our societies are highly dependent on the free and uninterrupted flow of large and invisible packets of information. Cyber space has become an important part of the world's economy, has led to a revitalisation of civil society, sparked revolutions, and helped governments provide better services to their citizens. However, the threats *to* and *in* cyber space as well as the threats enabled by cyber space have burgeoned.

Information has always been at the heart of security and defence strategies. Throughout the ages and across the world, the assured transmission of sensitive information has been one of the greatest priorities for leaders, particularly on the battlefield. As a

consequence, governments—and their opponents—turn to encryption to ensure information security in case of interception and decoding techniques to gain access to privileged communications. It can thus not come as a surprise that cyber space has become a new arena of confrontation. Just as crime and threats to national security are pervasive *offline*, they have begun to penetrate the world *online*. Cyber space has become a new "jugular vein" of modern societies, which must be protected or severed depending on one's point of view.

As a result, two new disciplines have emerged: cybersecurity and cyber defence. Both aim to protect against cyber attacks. Cybersecurity is a concern for everyone – from the individual over business world to the state. Cyber defence is the domain where the latter aims to counter actions by individuals, non-state actors, and even other states that threaten vital societal interests.

At the 7th International Cybersecurity Forum in Lille on 20 January 2015, French Minister of Interior, Bernard Cazeneuve, laid out the three cybersecurity challenges France needed to face: cyber defence to protect national institutions and interests; ensuring a high level of security of information systems across the public and private sector; and the fight against cybercrime.[1] Minister Cazeneuve argued that "[c]yberspace is now an arena with no border, where threats to our society are growing, since it is a tool that can be misused for malicious or criminal purposes by individuals and organisations. Within digital territories, as elsewhere, the State's responsibility is to resolutely protect citizens, anticipate threats, and suppress criminal acts when they occur. We must do everything we can to ensure that cyberspace is a place where fundamental freedoms are exercised and, I insist, the protection of privacy is guaranteed. […] Security in digital spaces must, therefore, be provided with as much determination as in our cities and all our territories."

For a long time, France has lagged behind its main strategic partners in cybersecurity and defence. However, in recent years, the country has undertaken considerable efforts to catch up to its peers, leading to conceptual reformulation, organisational reforms, and substantial increases in resources. These efforts are ongoing and have been stepped up recently.

Two recent cyber attacks highlighted the extent to which France needs to remain vigilant. The January 2015 terrorist attacks in France, which started with the attack against the *Charlie Hebdo* magazine, were accompanied by an unprecedented wave of cyber attacks on private and state web sites. Radical extremist hackers claimed more than 1,500 attacks in this period. A more symbolic cyber attack, however, was mounted on 8 April 2015 against the *TV5 Monde* television news channel, resulting in a blank screen and the dissemination of messages on social networks claiming to come from *TV5 Monde*, but supporting the so-called Islamic State.

This article provides an overview of the conceptual basis for French cybersecurity and defence policies, the most important elements of its organisational set-up, and recent cyber efforts and initiatives. The article does not claim to be exhaustive, but aims to provide a good starting point for related research.

Many French ministries and agencies are in one way or another involved in cybersecurity. To take but one recent example, the Ministry of Foreign Affairs created the position of a Cybersecurity Coordinator in October 2014. However, this article focuses on the efforts of the National Information Systems Security Agency (*L'Agence nationale de la sécurité des systèmes d'information*, ANSSI) and the ministries of defence and interior – the actors most heavily involved in French cybersecurity and defence.

The Conceptual Framework for French Cyber Policies

Cybersecurity and defence emerged as a distinct national security priority in France's 2008 White Paper on Defence and National Security.[2] Indeed, the White Paper singled out cybersecurity—together with nuclear deterrence, ballistic missiles, and nuclear-powered submarines—as a priority area for France "to retain its areas of sovereignty, concentrated on the capability necessary for the maintenance of the strategic and political autonomy of the nation." The White Paper identified large-scale attacks against information systems by state and non-state actors as a rising concern, singling out "cyber-war" as a "major concern." The White Paper mandated the development of a new concept for cyber defence and, notably, "the establishment of an offensive cyber-war capability."

In the wake of this strategic review, France steadily improved its cyber policies and capabilities, which were still very moderate at that time. A major outcome from the 2008 White Paper was the creation of new cybersecurity and defence institutions, most importantly ANSSI – the country's highest standing cybersecurity and defence agency, possessing national jurisdiction.

In 2011, ANSSI published France's first national cyber strategy, entitled Information Systems Defence and Security: France's Strategy.[3] It is still the guiding policy document for cybersecurity and defence. However, a new national cyber strategy is planned for release in the summer of 2015. The strategy lays out one big ambition and three core tasks. Through an enhanced cyber posture and co-operation with partners and allies, France aspires to "become a world power in cyberdefence" and belong to "the inner circle of leading nations in the area of cyberdefence." To achieve this goal, France must, first, safeguard its "ability to make decisions through the protection of information related to its sovereignty." In other words, state institutions need to be able to "communicate in any situation and in total confidence." Second,

given the growing importance of cyber space, the government must strengthen "the cybersecurity of critical national infrastructures." Third, the state must ensure a high level of security in cyber space *beyond* state and critical information systems. In other words, non-critical public service providers, the private sector, and citizens should be able to operate in a reasonably secure cyber space. The strategy identified seven areas where further actions were necessary:

- situational awareness;
- detection, alert, and response capabilities;
- scientific, technical, industrial, and human capabilities;
- protection of information systems of the state and operators of vital importance;
- adaptation of legislation;
- international cooperation;
- communication.

French cyber efforts over the last five years have been a drive for change in these areas. These efforts did not slow down with the change of president in 2012. To the contrary, strengthening France's position in cyber space remains an ambition that is shared by most political parties. Consequently, the focus on cybersecurity and defence was strengthened considerably in the new government's 2013 White Paper.[4]

The 2013 White Paper starts from the premise that "the continued growth of [the cyber threat], the continuing increase in the importance of information systems in the life of our societies and the very rapid development of technologies, require us to move onto yet another level to maintain the protection and defence capabilities responding to these changes." The strategic review thus argues for "a very substantial increase in the level of security and the means to defend our information systems." In fact, it states that France's ability to protect itself against and detect cyber attacks if they do occur, and identify the perpetrators has become an integral part of the way France exercises national sovereignty.

As a result of this analysis, the White Paper recommends strengthening the human resources devoted to cybersecurity and defence in order to reach parity with its British and German allies. It underlines the necessity of efforts to design and develop high-level security systems, supported by substantial budget allocations and paying special attention to electronic communications networks. Moreover, the government promises to build up the cybersecurity science and technology sector and industry. The White Paper also calls for an ambitious policy to protect the state's information systems by maintaining highly secure networks across state institutions, appropriate public procurement policies, and proper management of mobile communications

equipment. The policy is to be supplemented by awareness raising in decentralised state administrations, regional institutions, as well as the principal users of cyber space. Since a state's cybersecurity also depends on the security of its suppliers of goods and services, the White Paper furthermore mandates that clauses to that effect be inserted in contracts. Moreover, the White Paper promises that the government and parliament would define cybersecurity standards for operators of infrastructures of vital importance, spelling out their rights and responsibilities. The White Paper also recommends additional public awareness raising campaigns to change citizens' behaviour and habits. Computer security should furthermore be integrated into all higher computer technology education. As a consequence, all of these recommendations form a set of "cyber hygiene" guidelines. Lastly, the White Paper reaffirms France's support for the establishment of a European policy to strengthen the protection of critical infrastructures and electronic communications networks.

In order to safeguard against major cyber attacks, the White Paper conceptualises policy responses along two lines of effort. First, the government will implement "a robust and resilient posture to protect state information systems, operators of essential infrastructure and strategic industries." Second, the government will develop "a global and appropriate governmental approach" to cyber attacks. France will rely on diplomatic, judicial, and police resources as instruments of first choice. However, the government does not rule out "progressive use of Ministry of Defence resources in the event that national strategic interests are threatened." Interestingly, the language on offensive cyber capabilities was toned down in the White Paper, as compared to the 2008 version, referring obliquely to "a proactive IT capacity". This capacity would help define the threat and identify an attack's origin; make it possible to anticipate some attacks and configure defences accordingly; and give the government the possibility to scale response, depending on the magnitude and seriousness of the cyber attack. Despite the vague language, however, the Minister of Defence, Mr. Jean-Yves Le Drian, affirmed in June 2013 that he wanted to give France an "offensive IT capability," adding cyber attack capabilities to its land, sea, air, and nuclear weapon systems. He underlined that "what is at stake is the capability for remote control or destruction of vital infrastructure" and wants France to seek an offensive capability with "more or less reversible, more or less discreet resources, but always in proportion to the scale and gravity of the situation."

Organising for Cybersecurity and Defence

The National Information Systems Security Agency (ANSSI)

France has organised its cybersecurity and defence in a centralised manner in line with its historic state traditions, quite unlike the approaches undertaken by the United States and Germany for example.

As noted, ANSSI is the highest standing cybersecurity and defence agency in France. Reflecting the importance of cybersecurity in the eyes of the French state, ANSSI is under the direct authority of the Prime Minister. More precisely, ANSSI is part of the General Secretariat for National Defence and Security (*Le Secrétariat général de la défense et de la sécurité nationale*, SGDSN), which assists the Prime Minister in the exercise of his defence and security responsibilities and works closely with the Presidency of the Republic. ANSSI's current Director General is Guillaume Poupard.

Created in 2009, ANSSI succeeded the Central Information Systems Security Directorate (2001-2009) and the Central Cipher and Telecommunications Security Department (1986-2001). In 2010, ANSSI acquired the role of provider of cyber defence, in addition to the cybersecurity role mandated from its inception.

The agency's budget for 2014 amounted to EUR 80 mln, of which 30 mln were spent on salaries. At the end of 2014, the agency had over 420 employees, with the target of 500 employees by the end of 2015.

ANSSI's mission is four-fold: to detect and implement early reactions to cyber attacks; support the development of trusted products and services for state institutions and economic actors; advise and support state institutions and operators of vital infrastructure; as well as raise awareness and actively communicate on cyber threats.

The agency itself is divided into four sub-directorates.

- The Information Systems Security Operational Centre (Le Centre opérationnel de la sécurité des systèmes d'information, COSSI) is responsible for threat analysis; identification of vulnerabilities; and responding to ongoing cyber attacks by characterising the attack, designing countermeasures, and helping to resolve them. COSSI hosts the CERT-FR—the French Computer Security Incident Response Team (CSIRT)—and the Centre for Cyber Defence, which works closely with the Analysis Centre for Defensive Cyber Operations in the Ministry of Defence (Le Centre d'analyse de lutte informatique défensive, CALID).
- The Expertise Sub-Directorate (La Sous-direction Expertise, SDE) is responsible for maintaining ANSSI's science and technology expertise and applies it in-house and with its customers.
- The Secure Information Systems Sub-Directorate (La Sous-direction Systèmes d'information sécurisés, SIS) conceives, proposes, and delivers secure information systems for state institutions and operators of vital importance.
- The External Relations and Coordination Sub-Directorate (La Sous-direction Relations extérieures et coordination, RELEC) co-ordinates ANSSI's

relations with state institutions, the business sector, international partners, as well as the public.

Moreover, ANSSI can employ the Government Transmissions Centre, which assures the security of government communications.

As called for by the 2013 White Paper, the Military Planning Law for the years 2014-2019 (*La Loi de programmation militaire*, LPM) mandated explicit legislation on standards for cybersecurity, especially for government networks and private operators of vital importance. Operators of vital importance are designed by the French state and currently number over 200 operators. The French Defence Code defines these operators as "public or private operators which exploit some installations or use installations or facilities whose unavailability would seriously compromise the warfare or economic capabilities, the security or survivability of the nation." These operators "have to cooperate at their own expense […] in order to protect these installations, structures or facilities against threat, particularly terrorism." Through the LPM mandate, ANSSI could set mandatory security rules for the critical systems of operators of vital importance; should be notified of incidents occurring on critical systems of operators of vital importance; could mandate security inspections; and could mandate specific measures in case of major crises. These tasks were fulfilled with three ANSSI decrees released in March 2015.[5] This intrusive approach to operators of vital importance, in regard to cybersecurity, notably contrasts with approaches of many other states, which often work with industry-agreed standards and voluntary information sharing on cyber threats and attacks. Needless to say, the operators of vital infrastructure will have to spend substantial amounts of money on cybersecurity in order to meet these standards, but the French government believes that the benefits will outweigh the costs for French companies.

As already pointed out, one of the ways France implements willing to become a leader in cybersecurity and defence is through a vibrant cyber industry, which ANSSI is promoting comprehensively. In September 2013, the Minister of the Economy, Industry, and Digital Affairs launched the initiative "A New Industrial France."[6] The 33rd of the 34 plans of the initiative concerns cybersecurity. Led by ANSSI's Director General, the plan seeks to significantly increase the demand and supply for trusted cybersecurity solutions; help French cybersecurity companies capture larger shares of foreign markets; and strengthen French companies. One early outcome of this plan is the creation of the label *France Cybersecurity*, a label awarded to high-security solutions conceived and operated in France. In the beginning of 2015, the first 24 cyber solutions were awarded the label.

Ministry of Defence

The French Ministry of Defence (MOD) develops and operates complex information and communications systems, in particular those related to its most sophisticated weapons, such as the country's nuclear arsenal. The MOD therefore has its own cybersecurity and defence structures which work closely with ANSSI and other ministries charged with cybersecurity tasks.

Like many of its peers, the French MOD views cyber space as a military domain in its own right—next to the land, sea, air, and space domains—and is convinced that any future military operation will have a cyber dimension. The defence of cyber space is thus an ongoing necessity as the MOD needs to guarantee the effectiveness of the armed forces, the success of its missions, and the secure functioning of the MOD itself. The ministry took the cyber defence mission to heart in 2011 when it published the Joint Concept for Cyber Defence, defining the framework, principles, and required capabilities for military operations in cyber space. This was followed by the Joint Doctrine for Cyber Defence in which the MOD set down its organisation for cyber defence.

The Joint Doctrine created the position of a general officer in charge of cyber defence under the French Chief of Defence. The position is currently held by Rear Admiral Arnaud Coustillière who sits at the top of the operational command chain for cybersecurity and defence in the French armed forces. The "cyber general" fulfils two roles. First, he has an operational role in the Planning and Operations Centre (*Le Centre de planification et de conduite des opérations*, CPCO). In the CPCO, 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. Second, he is in charge of coordinating and developing cyber defence across the MOD as well as in the three services.

The MOD operates the CALID, which is in charge of surveillance, detection, and quick response in case of cyber attacks. In other words, it is the Ministry's CSIRT and thus works in close cooperation with COSSI, as well as with partner and allied military CSIRTs. Since February 2014, COSSI and CALID have been located in the same building in Paris, which makes the existing close relations between the two entities even easier to maintain.

On 7 January 2014, Minister Le Drian presented a new MOD cyber initiative. His Cyber Defence Pact aims to develop the MOD cyber capabilities and make them available to French society as a whole.[7] It has six lines of efforts with a total of fifty initiatives. The Cyber Defence Pact aims to:

- raise the level of information system security and the MOD's resources for cyber defence and military operations;
- scale up technical, academic, and operational research and supporting the French industrial base;
- reinforce human resources dedicated to cyber defence;
- further develop the Cyber Defence Centre of Excellence in Brittany;
- promote the emergence of a national cyber defence community;
- cultivate a network of foreign partners, especially in Europe but also within NATO and in areas of strategic interest.

The main challenge for the Cyber Defence Pact is the continuing lack of human resources. Financial resources are still insufficient to create new jobs, and the quality of training for applicants needs to be increased.

Two measures in the pact deserve closer attention: the Cyber Defence Centre of Excellence and the Citizen Cyber Defence. The MOD officially launched the Cyber Defence Centre of Excellence in February 2014. It is co-located with the Directorate General for Armaments for Information Security, which itself institutes important cyber efforts, and integrates the MOD's cyber skills in terms of training, research, and technology. The further development of France's cyber industry is another important aspect of the centre, as the government and local institutions aim to turn the Rennes region into a leading cyber hub in France and Europe. The Rennes region thus brings together a tight network among the Centre of Excellence, the Directorate General, the School of Signals, the Special Military School of Saint-Cyr, as well as universities and cybersecurity businesses.

Another innovative effort by the MOD, in collaboration with the French Gendarmerie, is the Citizen Cyber Defence (*Le Réseau cyberdéfense de la réserve citoyenne*, RCC), which provides a network of committed cyber experts. The RCC aims to make cyber defence a national priority through awareness raising programmes, bringing together professionals, advanced students, and students with expertise in the cyber field. It has six working groups:

- an "elected representatives and journalists group";
- a "youth group" for students and young professionals;
- a "development of citizen commitment group" (which contributes to discussions on a possible specific cyber defence reserve);
- a "think tanks and strategic thinking group";
- a "Small and Medium Enterprises/Industry group";
- a "big business group."

Ministry of Interior

The Ministry of Interior's work is naturally affected by the rising cyber threat, particularly with regard to its responsibilities to fight terrorism and crime. As its cybersecurity and defence tasks are not as clear-cut as they are for ANSSI and the MOD, Minister Cazeneuve created the position of a "cyber prefect" in June 2014 in order to bring coherence to MOI efforts. In January 2015, Jean-Yves Latournerie became the MOI's first cyber prefect under the direct authority of the minister.

The "cyber prefect" is in permanent contact with all parts of the MOI charged with some aspects of cybersecurity and defence as well as with counterparts in other ministries. His primary mission is to improve the MOI's institutional set-up on cyber threats – if necessary also through organisational reforms. He is also charged with creating synergies within the MOI and with integrating MOI cyber initiatives, ensuring they fit within the overall ministerial strategy. The "cyber prefect" also needs to ensure that the MOI strategy fits within European and international frameworks.

Several parts of the MOI maintain and important focus on the cyber threat. Chief among them are:

- the Directorate General of the Internal Security Forces;
- the Directorate General of the National Police, which has recently set up a Sub-Directorate on the Fight against Cyber Crime;
- the Directorate General of the National Gendarmerie, which has its Centre for the Fight against Digital Crime.

MOI cybersecurity efforts have also been strengthened by two initiatives in 2014 and 2015. In November 2014, the government enacted a law that strengthened its counterterrorism efforts. Most importantly, the fight against using the Internet for destabilisation has been stepped up, e.g. by introducing the notion of a "threat *through* cyber space." The law also put into place cybersecurity provisions such as "cyber patrols" against organised crime; the introduction of digital data theft as a criminal offence; harsher penalties for organised gang attacks on automated state data processing systems; the facilitation of computerised data searches and decryption of encrypted data.

In January 2015, the Minister of the Interior also clarified the MOI cybersecurity and cyber defence policy, submitting an action plan built around six strategic lines of effort.[8] First, to achieve full situational awareness, the "cyber prefect" will issue an annual report on cyber threats and set up an appropriate statistical system to measure cybercrime.

Second, the MOI will strengthen its analytical and operational response capabilities, particularly through synergies and information sharing. More broadly, the fight

against cyber threats is part of the MOI's plan for modernisation. The MOI will spend over EUR 100 mln between 2015 and 2017 on equipment for the internal security forces, and one element is to modernise and secure the MOI computer networks.

Third, better awareness raising campaigns and public communications are further objectives. The Directorate General of the Internal Security Forces already works directly with operators of vital importance and the most strategic companies, and the Gendarmerie concentrates on small- and medium-sized enterprises and industries and integrates new cyber threats into its awareness programmes. Preventive measures for the French youth are also an MOI priority, for example through the "Internet Licence" programme for students leaving primary school.

Fourth, research and development on cybersecurity is to be strengthened. The MOI links up with the other ministries that promote the industrial base for trusted cybersecurity solutions. In line with ANSSI's actions under the "New Industrial France" initiative and as part of the work within the committee of the security industries sector, the MOI thus aims to support the emergence of a French and European cybersecurity sector.

Fifth, the MOI wants to raise the security level of its own information systems. This involves, inter alia, ensuring that all staff are made aware of the challenges of information system security and providing them with trusted tools and systems, especially for mobile use.

Sixth, the MOI promotes international action with foreign partners and allies under the coordination of the Directorate General for International Cooperation. For example, in 2014 nearly 300 foreign partners benefited from MOI expertise on cybersecurity.

Conclusion

After the cyber attacks on Estonia in 2007, France came to realise that it had fallen behind the countries that it normally compares itself to when it comes to security and defence: the United States, the United Kingdom, and Germany. It thus set out a path to remedy this situation through concerted efforts to increase its national cybersecurity and defence capabilities and to seek more effective international co-operation and coordination, in particular with the European Union and NATO.

While France has come a long way in terms of its cyber policies, organisation, and budget, the continuing rise in attempted and successful cyber attacks means that these efforts have been only a start. Much more needs to be done across the public and private sectors. The budget allocated to counter the cyber threat will play a big role. In times of austerity, holding the line or ever increasing budgets for security and defence

is difficult – to say the least. However, France has realised that its national sovereignty would be undermined irreparably if it does not allocate the necessary financial resources. One positive sign in this regard is the adoption of a modified LPM for the years 2015 to 2019, which was passed in April 2015. The modified LPM continues the strong focus on cybersecurity and defence, most importantly promising an additional EUR 1 bln on cyber defence and the creation of 500 new jobs in cyber defence. In short, the current level of the cyber threat, the political commitments across party lines, and the necessary money behind the cybersecurity and defence drive all bode well for French cyber efforts. The next big step will be the adoption of the new national cyber strategy, which the Prime Minister plans to publish in the summer of 2015.

Notes:

[1] Bernard Cazeneuve, at 7th International Cybersecurity Forum, Lille, 20 January 2015, "FIC2015 Discours de Bernard Cazeneuve et Thomas De Meziere," International Forum on Cybersecurity, accessed on 16 July 2015, video available at https://www.youtube.com/watch?v=v9NPGaVHqmU.

[2] President of the French Republic, *The French White Paper on Defence and National Security*, 2008, accessed on 16 July 2015, available at http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf.

[3] Prime Minister of the French Republic, *Information Systems Defence and Security: France's Strategy*, 2011, accessed on 16 July 2015, available at http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

[4] President of the French Republic, *The French White Paper: Defence and National Security*, 2013, accessed on 16 July 2015, available at http://www.rpfrance-otan.org/IMG/pdf/White_paper_on_defense_2013.pdf?572/67a412fbf01faadf4bbac1e9126d2e32f03f0bc0.

[5] See "Communiqués de Presse," ANSSI, accessed on 16 July 2015, available on http://www.ssi.gouv.fr/presse/communiques-de-presse/.

[6] Government of the French Republic, "La nouvelle France industrielle: Présentation des feuilles de route des 34 plans de la nouvelle France industrielle," accessed on 16 July 2015, http://www.economie.gouv.fr/files/files/PDF/nouvelle-france-industrielle-sept-2014.pdf.

[7] Ministry of Defence of the French Republic, "Pacte Défense Cyber: 50 mesures pour changer d'échelle," 2014, accessed on 16 July 2015, available at www.defense.gouv.fr/content/download/237702/2704402/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf.

[8] Bernard Cazeneuve, at 7th International Cybersecurity Forum.

PHILIPPE VITEL is member of the French National Assembly for "Les Républicains" (The Republicans), first elected in the 2nd constituency of Var in 2002. He is on the National Defence and Armed Forces Committee in the National Assembly, where he was the co-author of the information reports on the execution of the Ministry of Defence's budgets in 2011, 2012, and 2013, as well as on France's maritime operations in 2012. He also authored an opinion on a defence partnership between France and Gabon in 2011. As a member of the French delegation to the NATO Parliamentary Assembly, he is the Special Rapporteur of the Science and Technology Committee and member of the Ukraine-NATO Inter-parliamentary Council. In 2014, he authored the report on *Cyber Space and Euro-Atlantic Security* in the Science and Technology Committee. Mr Vitel is a former plastic surgeon.

HENRIK BLIDDAL is Director of the Science and Technology Committee at the NATO Parliamentary Assembly since February 2011. Since October 2013, he is also the Director of the Research Assistant Programme at the Assembly. He graduated in Political Science from the University of Copenhagen, Denmark. Among others, he is the author of "Reforming Military Command Arrangements: The Case of the Rapid Deployment Joint Task Force," Letort Paper (Carlisle, PA: Strategic Studies Institute, US Army War College, 2011) and co-editor of *Classics of International Relations: Essays in Criticism and Appreciation*, eds. Henrik Bliddal, Casper Sylvest and Peter Wilson (Abingdon: Routledge, 2013). He is the former editor of the multidisciplinary social science journal *Politik* at the University of Copenhagen. His research interests include cybersecurity and defence, the organisation of national security and defence, and emerging security challenges. *E-mail*: hbliddal@nato-pa.int