Compte-rendu[1]
du Colloque de recherche

Cyber-security:
Innovation, Regulation and Strategic Shifts

Organisateur: Pr. P. Baumard,
Ecole Polytechnique, Chaire IRSN

Chaire Innovation & Régulation des Services Numériques
Ecole Polytechnique - Telecom ParisTech - Orange

November 21st 2012, Ecole Militaire, Paris

Table des matières

Contre-Amiral Arnaud Coustillère, Officier Général de Cyber-Defense, Etat-Major des Armées. : « Opérer en sécurité dans le cyberespace. » 1

JP Macintosh, UCL, "Of resilience of irresilience : fitness for the strategic shifts of cyber environments" 3

Dr. Chris C. Demchak, Professor Strategic Research, "Socio technical, systemic survival in the emerging cybered conflict age" 4

Mr. Jean-Luc Moliner, Senior Vice President, Security, France Telecom-Orange Threats, Trust, technology. 5

John Mallery, Research Scientist, MIT Computer Science and Artificial Intelligence Laboratory, "strategic considerations in cyber defense: leverage, coordination, norms and policy. » 9

Mr. Cédric Blancher, Senior Expert Cyber-Security Expert EADS Group. "Back to the Field" 10

Philippe Baumard, Professeur, chaire innovation & régulation, Ecole Polytechnique. "A Triangular Evolution: Doctrines / Regulation / Innovation » 12

Contre-Amiral Arnaud Coustillère, Officier Général de Cyber-Defense, Etat-Major des Armées. : « Opérer en sécurité dans le cyberespace. »

Officier en charge de la cyber défense à l'État-Major des armées depuis 2011, il dirige une fonction nouvelle qui a nécessité la réorganisation de l'ensemble du processus opérationnel. Le but de l'intervention est de montrer un scénario intéressant, possible et plausible, afin de montrer que sur un scénario simple, la déstabilisation d'un État est possible. Ce genre de scénario permet de savoir comment contrer une crise et une attaque. Il suppose une planification globale en vue de leur enchaînement cohérent pour déstabiliser fortement la France ; une organisation très bien structurée ; et d'avoir mené au préalable des actions discrètes de renseignement (cyber et non cyber).

Les **stades d'une attaque possible sont :**

Décrédibilisation de l'État

[1] Ce compte-rendu bilingue a été réalisé avec l'aide d'Olivier Milovanovitch, Ecole de Guerre Economique, Paris, que nous remercions. Chaque synthèse a été réalisée dans la langue d'expression du paneliste pendant la conférence.

Manipulations et provocations sur les réseaux sociaux.
Perturbations des sites étatiques (institutions, formalités en ligne, paiements).
Attaque de déni de service et défacement.
Perturbations des opérateurs GSM

Désorganisation de la société surtout des systèmes vitaux.
Perturbation des capacités de transports des opérateurs nationaux et des accès internet
Attaques massives répétées des réseaux bancaires ou de distribution d'eau
Perturbation des réseaux électriques provoquant des black-out et incidents en chaînes ;

Fragilisation des PPS
Ce type d'attaque est une réalité quotidienne dont le monde militaire n'est pas à l'abri. Bien que des attaques puissent gêner la bonne marche des systèmes et des organisations, cette cybercriminalité n'est pas la plus préoccupante. Ainsi existe-t-il des attaques à des fins stratégiques contre des individus et des organisations d'ampleur et de discrétion variables, fruit d'une préparation et de cibles précises, voire d'actions préliminaires dormantes. Ce sont des actions discrètes. Par exemple : l'utilisation d'outils informatiques tels stuxnet a été mise en place par des organisations fortement préparées sur une cible donnée et à temps précis. Ce type d'outils nécessite une très forte organisation.

Fort du constat que l'on voit émerger un véritable cyberespace avec des acteurs très variables ainsi qu'une dilution des frontières, l'enjeu de l'officier est d'accompagner la numérisation de l'espace de bataille. Le cyberespace ne doit pas rester un endroit où tout est permis. L'Officier Général de Cyber-défense définit le cyberspace comme un espace de communication constitué par l'interconnexion mondiale de systèmes de traitement automatisé de données numériques. C'est un lieu d'échange d'idées, de services et de biens.

L'Officier Général de cyber-défense propose comme typologie des attaquants : Le cybercrime / Le cyberactivisme / Les cyber-organisations étatiques ou non. La complexité de l'attaque va croissante en fonction du degré d'organisation. L'Officier Général identifie notamment le manque de vigilance des utilisateurs du cyberespace comme principal risque. Les comportements humains ont été sous-estimés au bénéfice des moyens et éléments techniques. Désormais : le but est d'éduquer le personnel des organisations à faire preuve de prudence. L'Officier Général de cyber-défense fait un parallèle entre le droit du cyberespace et le droit maritime en prenant comme exemple la piraterie. Le cyberespace est omniprésent : dans les avions, les chars, les navires. Ces systèmes doivent être utilisés en minimisant les problèmes de sécurité.

Les actions malveillantes portent sur les systèmes d'armes et l'informatique embarquée dans le système d'arme ainsi que sur la sécurité des documents classifiés et Sur les infrastructures et les plateformes de combat (SCADA). La coopération est le seul moyen de lutte viable. C'est la raison pour laquelle le SGDSN/ANSSI et le MINDEF en font une priorité.

Une organisation renforcée nécessite une mise en place d'un commandement opérationnel unifié, centralisé, spécialisé pour la défense active des SI., c'est-à-dire capable de mobiliser l'ensemble des moyens nécessaires pour limiter les dommages, avec une très forte capacité d'action. Quatre équipes de quatre personnes constituées en 24h sont mobilisables partout en France.

Formation du personnel : un axe majeur à accélérer. La priorité est le développement d'un esprit de cyber-sécurité : comportement sain ou « hygiène cybernétique ». Il s'agit d'une compétence spécialisée de filière. Elle nécessite une formation au commandement et à la conduite « cyber ».

Réseau citoyen de cyber-défense (RCC)
Transposition du concept d'armée nation. Liens avec des citoyens préparés.

JP Macintosh, UCL, "Of resilience of irresilience : fitness for the strategic shifts of cyber environments"

JP Macintosh wishes that cyber-policies involved less thinking and more doing and learning. He begins his intervention asking **"**who would count themselves as empiricists?" and points out that **beside** Maritime, land, space and earth there is another environment called "cyberspace" which is not unreal.

Crises are decisive moments and explain why people confuse "crisis" and "catastrophes". The answer is simple: bureaucrats are not educated to think beyond the case. The ways they handle crisis are not appropriate. This would turn crisis into catastrophes. But crisis are decisive moments, turning points for better or worse. He defines the concept of "Resilience" as the enduring power of a body or bodies for transformation, renewal and recovery through the flux of interactions and of events. He binds competitiveness and resilience. If a society is not resilient, it is not competitive. This is the reason why a doctrine is needed. For Dr. Macintosh, most "irresilience" is self-inflicted.

Dr Macintosh points out that the more you do the more complicated life gets. He insists about the importance of having and education on what matters. His principal question remains: how can we gain productivity thru crises. The answer lies in crafting strategies of resilience that integrate crises as opportunities for engaging beneficial changes. But what are such strategies?

Strategies are not
Thinking & making drafts
Rhetoric, wish lists or easy to measure targets
Well-articulated public policies
A really big plan
Communication public relations
The monopoly of the military over security

Strategy is
Ends and means and ways
Consumption rate attrition; enabling ways
Anticipating the afterthought
Including others and the environment

The key issue is to find the competitive option focusing on decision takers. For example, the winning contributions to the Cold War acknowledged heterodox economics. Hence, a sound

cyber-security strategy must encompass the key components of Behavioral economics, Organization theory, and evolutionary economics.

Dr. Chris C. Demchak, Professor Strategic Research, "Socio technical, systemic survival in the emerging cybered conflict age".

Every conflict in the future will have a part of cyber. Now all opponents of any sovereign state have historically new choices in scale, proximity and precision to create an inventory of attacks for little cost. As a result, they get a wide range of conceivable forms of cybered conflicts. Dr. Demchak reminds the audience that the global Internet is a global substrate of multitudes of **socio technical systems based on trust.**

A Cyberspace imposes several layers of surprise sources: Basic large organization surprise (routine complexity in large STSS) ; connected Cybered critical infrastructure; and with Web access Anywhere – a now threatened whole socio-technico-economic system. The problem remains in a fourth layer where wicked actors get through cyber defenses.

To become a cyber-power a country needs both resilience and disruption. The strategy emphasis includes Local Responsibility; CIP/CEP infrastructure and Economic links; Crisis management, which requires both persuasion and voluntary regulation. In such an arena, "bad actors" require legal pursuit; cybercrime laws and channeled tracking efforts at international cooperation. Tailored Disruption (trace backs, broad monitoring over mass data, coming in or outside existing borders)

Democratic leaders need to acknowledge that:
Knowledge is the source of security
States need resilience AND disruption capacities in a balanced security resilience Strategy
Not everyone wants a civil society.
There are no natural frontiers in cybered-conflicts, but cyber-space encounters divisions.

Cyberspace is already being divided. Nations and many firms erecting greater controls on electronic inputs out of frustration and fear for themselves in bits and pieces. Control on bad inputs buys slack in time when surprise and borders historically make slack for a nation, a community and even a home. But borders are now Emerging in Cyberspace**.**

Several **questions shall be answered:** Framing: what kind of institutions do we want? Instantiating: Who has to design those technologies? Will the relative resilience of nations be a part of state responsibility? What are the models best practices and advanced learning mechanism available for the critical institution to maintain stability.

Governments are learning to play by the Bad and Wicked Actors Rules. A mutual security resilience shield could be the solution because it offers more efficiency, lower the burden on each of us by reducing the ease and effectiveness of criminal attacks, prevents endless replays of same attacks, and reinforces attention to all four layers.

Mr. Jean-Luc Moliner, Senior Vice President, Security, France Telecom-Orange Threats, Trust, technology.

Cette intervention se place sous 2 angles qui sont : L'aspect Sécurité d'une entreprise qui travaille dans les télécommunications, qui fabrique des autoroutes de l'information et aussi des stations services auxquels les utilisateurs se raccrochent lorsqu'ils sont sur internet ; En tant qu'opérateurs « d'infrastructures vitales », nécessairement en contact avec l'Etat.

« La réalité du champ de bataille est qu'on n'y étudie pas; simplement on fait ce que l'on peut pour appliquer ce qu'on sait. Dès lors pour y pouvoir un peu, il faut savoir beaucoup et bien » F. Foch à l'Ecole de Guerre, 1903. Cette citation résume bien ce que l'on vit aujourd'hui à l'intérieur des entreprises en termes de lutte permanente contre les activités criminelles (ou autres) autour du cyberespace. Effectivement on fait ce que l'on peut, on applique ce que l'on sait au moment où l'incident se passe mais cela nécessite surtout que l'on connaisse à la fois l'infrastructure, le système en temps réel et tout cela, sans avoir recours à une myriade de sous-traitants.

Cette présentation s'articule en 3 parties (2 interrogations et une lueur d'espoir !). Quel est, aujourd'hui, le niveau de la menace pour les entreprises (mais aussi pour les Etats par le biais des infrastructures vitales)? Quelles seraient du point de vue des entreprises, les mesures à prendre pour restaurer la confiance ? La présentation se conclue par un parallèle avec le cas de la sécurité dans le domaine de l'automobile. Quel est le niveau de la menace ? La nature de la menace est différente pour les Etats et pour les entreprises.

Pour les Etats , à ce jour, la cyber menace seule n'est pas de nature à mettre à genou un Etat, bien qu'elle puisse créer des problèmes dans le tissu industriel et donc, par répercussion, des problèmes économiques ou sociaux. Par comparaison, les catastrophes naturelles (tsunami, incendies) sont plus dangereuses pour tester la résilience des Etats que les attaques informatiques. Les études faites par les opérateurs télécoms ont montré que les attaques peuvent perturber le fonctionnement des systèmes de communications de manière assez significative. Du point de vue d'un Etat, neutraliser tous les opérateurs d'un pays au même moment pour une période longue semble un objectif difficile à atteindre pour un adversaire potentiel.

Il est souvent cité l'exemple de l'Estonie, bien qu'il soit un petit pays en termes de complexité cybernétique. A titre de comparaison, France Telecom a environ 10 000 fois plus serveurs que ce pays. La complexité croissante des systèmes d'information des cibles à attaquer, déconnectés de toute notion de territoire (avec des serveurs dans 170 pays) retarde considérablement les attaques puisqu'une simple cartographie de l'ensemble des systèmes est un travail conséquent. La manœuvre pour arriver à l'objectif est importante. Il ne faut pas non plus négliger les effets collatéraux de l'attaque et en particulier l'effet boomerang. Exemple des codes de Flame ou Stuxnet qui ont été largement propagé dans le milieu underground.

Pour contrer ces attaques, de nombreux Etats ont développé des réseaux totalement indépendants par rapport à Internet et donc isolés de possibles attaques sur ce réseau. C'est la menace à moyen et à long terme auquel il convient de porter le plus d'attention : Il faut que les Etats pensent leurs infrastructures critiques au niveau national mais surtout au niveau supranational et envisagent l'ensemble de leurs infrastructures comme un « système de systèmes ». Cela nécessite un Etat qui soit à la fois architecte, normatif et volontariste.

Au delà du niveau de la menace que l'Etat doit fixer, on doit pouvoir adopter une méthodologie de réduction des risques. A qui doit s'adapter cette méthodologie coordonnée et qui doit être appliquée? A l'évidence avec des acteurs du secteur privé puisque l'Etat ne peut s'en sortir seul. Il est également nécessaire de coordination la dépense publique et privée de manière intelligente.

Au sein des potentiels dégâts engendrés par une attaque, ce sont les dommages indirects qui sont les plus importants : en particulier les effets « cascades » non maîtrisés (pour l'attaquant comme pour le défenseur). Deux exemples :

- des effets cascades de la panne du 6 juillet où le réseau télécom (11 heures)
- des DDos sur des sites étrangers et qui rebondissent jusqu'à la France.

Qu'en est-il de « l'internet des objets », très évocateur pour le grand public ? Sa plus grande faiblesse est qu'il est mono-technologie (entièrement basé sur l'IP). La résilience étant aussi facteur de la diversification des technologies, c'est une technologie dont les risques doivent être mesurés. Il reste également un travail conséquent pour gérer les possibles fraudes comme pour l'arrivée de tout nouveau système. Dernier aspect pour les Etats, la menace de l'espionnage : Ainsi il se peut que lors de sommets internationaux, les participants étrangers semblent disposer d'un script identique à ceux des participants français. A ce sujet, c'est une éternelle course-poursuite entre la sécurité et les nouveaux moyens d'attaques.

Pour les entreprises, les conséquences sont aujourd'hui plus graves, car elles sont plus exposées, plus menacés. Elles ont donc une nécessité d'agir. Il existe 2 types de menaces :

- *Le harcèlement* : se rapprochant d'une maladie chronique pour les entreprises partout dans le monde. Il se manifeste quotidiennement par des attaques DDOS, fraude, vol de données, manipulation de données techniques (y compris par de grands opérateurs !). Ce monde est comparable à un monde de voyous. Toutefois, les entreprises ont appris à gérer ce bruit de fond.
- *L'espionnage :* risque beaucoup plus sérieux pour les entreprises car contrairement aux Etats « immortels », les entreprises ne le sont pas. Les activités d'espionnage sont menées soit par des Etats, soit par des cyber-corsaires (qui peuvent être éventuellement financés par des Etats…).

Pour ce type de méfaits, les entreprises ne sont pas conçues pour contrer ces menaces. Les entreprises à haute valeur technologique en particulier ne sont pas prêtes à faire face à des attaques ciblées sur le long terme. Exemples de l'utilisation du Social Engineering (qui flattent l'égo de salariés). Les objectifs de ces opérations sont de capter le plus longtemps possible de l'information auprès d'une ou plusieurs personnes ciblées. Au-delà de la perte financière, les entreprises doivent faire face à un affaiblissement de leur compétitivité. A cet égard, on peut se demander pourquoi les comités exécutifs ne sanctionnent pas d'avantages les manquements dans ce domaine ?

Seule la prise en compte de la cyber sécurité dans la gouvernance des entreprises (au niveau des conseils d'administrations et des comités exécutifs) avec l'instauration de mécanismes incitatifs et punitifs permettrait de rééquilibrer les arbitrages financiers au profit de la sécurité, comme cela a été fait dans le domaine de l'éthique ou de la responsabilité sociale d'entreprise.

Quelles sont les mesures de confiance envisageables ? Au niveau international, les entreprises ne demandent qu'à être plus rassurées par les Etats. Elles souhaiteraient qu'une initiative diplomatique puisse aboutir à un traité de non militarisation du cyberespace. Les manœuvres dans le cyberespace réduisant la confiance des entreprises ce qui a terme nuit l'ensemble des acteurs de l'économie mondiale. Fin 2011, une proposition russe sur la cyberguerre a été rejetée par les Etats-Unis qui préféraient se concentrer sur l'angle de la lutte contre la cybercriminalité.

Quelque soient les décisions prises par les Etats, les infrastructures critiques, majoritairement supportées par des entreprises privées, ne sauraient résister à des attaques d'Etats manipulant le cyberespace. A titre de comparaison, le traité sur l'utilisation pacifique de l'espace extra-atmosphérique de 1967, est entré en vigueur tout juste 8 ans après le lancement de Spoutnik. Il existe donc au moins un exemple histoire où des Etats se sont mis d'accord pour gérer la neutralisation temporaire de l'espace.

Il faut espérer qu'un traité sur le cyberespace prendra moins de temps à signer que celui sur l'espace maritime qui prit plus de 400 ans. Un préalable à un traité est une prise de conscience par les Etats de la nécessité de négocier. A ce titre, une attaque ciblée sur les infrastructures d'un pays habituellement belligérant pourrait le pousser à considérer qu'il a plus à perdre qu'à gagner en commettant ce type d'actes… Les 5 à 10 ans à venir pourraient voir débuter des discussions sérieuses d'un tel traité. Citant M. Hague, le ministre britannique des Affaires Etrangères, le débat se situe sur la frontière entre la liberté d'expression et la notion de souveraineté.

L'espionnage étant la forme d'attaque la plus dangereuse pour les entreprises comme pour les Etats, il existe une nécessité de savoir en interne (contre-espionnage traditionnel) et en externe (dans l'underground ou dans les réseaux des Etats peu regardant). Malgré les efforts consentis, la France est encore loin d'avoir une vision internationale du sujet (Ukraine, Russie, Chine, etc.).

Au niveau de l'écosystème industriel ; il existe quelques pistes d'actions. Sur les normes techniques : pour l'IPV6, les garanties sur la sécurité ne sont pas assurées à certains endroits de la chaîne. Les fondamentaux de la sécurité ne doivent pas être en option sur ce sujet comme sur d'autres. Au niveau de la gouvernance des entreprises : la sécurité doit être prise en compte comme l'éthique ou la RSE. Au niveau de la législation comme par exemple la lutte contre les botnets : Les opérateurs savent quels sont les ordinateurs infectés par le botnets néanmoins la loi leur interdit de prévenir les utilisateurs infectés.

Au niveau de la sécurisation de la Supply Chain : comment une organisation peut s'assurer que les équipements qu'elle achète ne sont pas ouverts à tous vents ? Une évaluation de la menace par la Grande-Bretagne a été effectuée, celle-ci manque en France et en Allemagne. Les britanniques obligent désormais tout fournisseur d'une infrastructure vitale de l'Etat à transmettre le code source de sa technologie pour que celui-ci soit analysé par des citoyens habilités confidentiel défense. Cette méthode a le mérite de la clarté. Lorsqu'on leur demande, Huawei fournit le code source de ses produits, ce que d'autres fournisseurs refusent… Il faut donc dépasser la seule notion de coût pour prendre en compte les risques associés à l'achat provenant de pays tiers. On aborde ici, la question de la confiance qu'on accorde à ses partenaires, au niveau des Etats comme au niveau des entreprises.

Enfin, la problématique de **l'ingénierie des systèmes pour les opérateurs d'infrastructures** vitales : les tests de robustesse sont moins pratiqués au détriment des tests fonctionnels (de charge par exemple) pour des notions de coûts et de temps de développement.

Le cas de la sécurité dans le domaine automobile : L'accident dans le domaine automobile et l'incident dans le domaine informatique sont toujours définis comme des événements fortuits et pourtant ils ne sont pas inéluctables. Il existe un grand nombre de moyens pour lutter contre ces phénomènes. L'Union Européenne s'était fixée l'objectif de réduire de moitié le nombre de tués sur les routes entre 2001 et 2010. La réduction n'a été que de 43% ce qui est tout de même encourageant. Pourquoi ne pas avoir des objectifs comparables en termes d'incidents dans le système d'information ?

Cette réduction est le résultat d'un effort structurel des constructeurs basé sur la sécurité passive et active : **Sécurité passive** implémentée au travers du désign et des fonctionnalités. Entre 1910 et 1950, on a développé des fonctions liées à la vision (rétroviseurs, essuie-glaces…), mis en place des systèmes hydraulique de frein, d'assistance au freinage, améliorer la tenue de route et l'adhérence (pneumatiques). Et **sécurité active** avec comme enjeu la protection des occupants ce qui a été fait avec des procédés de déformation des structures, l'utilisation des crash-tests, l'invention de l'airbag… puis enfin un travail sur les piétons. La médiatisation a été un facteur puissant d'évolution des constructeurs dans le domaine de la sécurité.

On a également inventé la **sécurité prédictive** (l'ABS, l'ESP, éclairages halogènes et LED). Tout ceci a été fait à prix constant. Quels enseignements peut-on tirer de ces évolutions dans le domaine automobile? Un rôle majeur des clients au travers de la sensibilisation et de la médiatisation ; une démarche permanente des constructeurs pour développer une sécurité structurelle ; une sécurité passive qui permet de maîtriser l'outil ; une sécurité active pour limiter les dégâts ; une sécurité prédictive pour éviter les obstacles ; et surtout un basculement des concepts marketing dès le premier choc pétrolier de 1973 (vers la sécurité au détriment de la vitesse et du toujours plus…)

Et dans le domaine de la cyber-sécurité ? La cyber-sécurité vit dans un paysage industriel éclaté qui utilise des systèmes hétérogènes avec une sécurité structurelle faible voire inexistante. La sécurité passive est encore non exploitée et doit être développée en mettant en place des systèmes de logs et de sondes pour détecter. Il n'existe pas non plus de crash tests normalisés dans le domaine des infrastructures. La sécurité active est chère et difficile à intégrer et sous-utilisée. Une sécurité prédictive basée sur des systèmes de comportements encore balbutiants.

Alors que l'automobile nous a montré la voie, il faudra mettre en place dans le domaine des SI, un écosystème industriel basé sur des intégrateurs capables de gérer l'évolution complète de systèmes sur les couches réseaux et sur les couches applicatives. C'est donc forcement une intégration verticale par des grands groupes soutenu par un tissu de PME innovantes. Les principes de la guerre sont-ils utilisables dans cet espace temps ? Peut-on espérer la victoire sans bataille ? Peut-on vaincre sans assumer des pertes potentielles? Peut-on subir une surprise stratégique dans ce domaine ?

John Mallery, Research Scientist, MIT Computer Science and Artificial Intelligence Laboratory, "strategic considerations in cyber defense: leverage, coordination, norms and policy. »

National and economic security demands robust responses. Cyber arms control means defensive complexity analysis provides leverage; prioritization and measurement remains one of the key problems in defense coordination

Global ICT capital goods have evolved in such a way that they contribute to exporting cyber insecurity. Cyber-insecurity thrives on architectural vulnerabilities that are driven by a dangerous tolerance towards market failures. The United States has never done better in protecting the homeland and key infrastructures. Yet, we still need architectures that are secure by design. One of the key issues lies in the misaligned incentives. As a consequence, proliferating technical attack surfaces and vulnerability rises from a systemic misallocation of risks. Professor John Mallery presents several key elements where he believes there is much room for improvement, followed by key recommendations.

The national security argument for urgent action: accelerating instability in international security systems. There has been an erosion of post war international security architectures. Consequences of erosion: adversaries have found new ways to push their ideas forward. Only solution is to simplify complexity.

Concept of proportional judgment: Monotonous and monolithic policies increase intrinsic risks. A multilevel cyber deterrence strategy is critically needed. One of the core priorities is to engage in digitization that are not any longer using 'unsecurable' and 'indefensible' technologies.

Cyber arms control: Cyber-arm control is too often grounded in one single policy that aims at making offensive techniques obsolete. The problem is that countering cyber erosion does not lead towards strategic stability. Hence, the remaining solution is to raise the assurance level, which often leads to a partial covering of risks.

Mitigations vs. solutions: The threat mitigation domain can only cover near term risks. A sound cyber-security policy requires long-term solutions. An effective defense must be faster than the exponential proliferation of threats for a net defensive work factor. Hence, the role of a *transformational defense* is to outpace both threat and vulnerability curves.

Threat actors and capabilities: threat actors use a lot of the defendants' resources. We are facing multi-spectrum adversaries, which encompass nation states, high-end cyber crime, remote access and insiders, supply chain trusted connection domain partners.

Defensive complexity analysis: Response to cyber asymmetries requires high leverage solutions. The security meta-metrics focus on the difficulties met by attackers or defenders' basics dimensions. Work factors make technical or policy moves that cumulatively reduce the likeliness of a successful attempt. It increases the adversaries' uncertainty. This analysis has to take into account the cultural dimension.

High leverage solutions: They eliminate whole classes of vulnerability by design, i.e. by fixing security vulnerabilities at their source retires an entire attack surface and its

consequences. Leverage means fixing the cause rather than the symptoms (e.g. role of lack of separation of operating systems such as tree-structure systems)

International data exchange and collaborative analysis: Attackers can replay attacks across different countries. The international role of data exchange is critical. Information sharing and defensive coordination can reduce asymmetries of cyber attack and defense.

Defensive complexity analysis: Coordination reduces search space for defenders. Attackers search any possible leverage. A better work on the life cycle of critical infrastructure can lead towards a non-proliferation regime. States are responsible for trustworthy core national telecommunications infrastructures, as well as for cyber norms. States should seek to foster enabling market mechanisms to raise national information assurance, while monetizing their cyber security, and modernizing the ICT sector.

To conclude, Professor Mallery highlights the role of effective national cyber responses, which must overcome microeconomic interests oblivious to national security and wellbeing.

Mr. Cédric Blancher, Senior Expert Cyber-Security Expert EADS Group. "Back to the Field"

Le discours qui tend à montrer que l'on pouvait gérer les attaques passées mais que, aujourd'hui, les attaquants nous dépassent est faux. Les techniques utilisées dans les attaques sont stables, et il n'y a pas de « révolution technique » notable dans les familles d'attaques observées. M. Blancher montre à l'écran deux attaques, espacées de 3 ans, et visant un grand groupe industriel français. La première consiste en un mail envoyé en petit nombre à un service financier ciblé d'un grand groupe français. L'auteur se disait être la Directeur de la Communication Financière (accompagné de 2 documents .doc). La seconde est tout à fait similaire, bien qu'âgée de 3 ans. Dans les deux cas, la pièce jointe contenait un mécanisme d'exploitation de vulnérabilité du système de protection (« exploit »), mais les techniques sont tout à fait similaires. Ce sont toutes les deux des « Advanced Persistent Threats » (menaces avancées), mais le caractère « avancé » réside dans la campagne, le masquage, la façon dont sont amenées ces communications au cœur de la cible, et non pas dans les techniques utilisées pour perpétrer l'attaque.

Le constat que l'on peut tirer de cet exemple est simple : dans l'industrie de l'informatique ou de la sécurité, les gens n'apprennent pas énormément ! L'industrie de la sécurité n'est pas évolutive. Les améliorations que l'on a connues dans la dernière décennie sont incrémentales (pas d'innovation de rupture). Nous sommes passé de l'IDS (détection d'intrusion – en vogue dans les années 2000) à IPS. Il s'agit plus d'un recyclage de vieilles techniques qui ne fonctionnent pas (ou pas bien) et qui ne résout pas le problème des faux positifs.

Le stade de complexité sur les infrastructures informatiques est affolant. L'accroissement le plus significatif a eu lieu ces dernières années. Dans l'industrie, que ce soit en Europe, aux Etats-Unis ou ailleurs, personne ne semble capable de simplement dire « comment ça marche ». Cet état des lieux n'est pas la conséquence d'une inadaptation des savoir-faire techniques, mais bien la conséquence du modèle économique de l'industrie informatique qui privilégie l'ajustement permanent par l'ajout de couches complexes, sans un travail en profondeur sur l'innovation fondamentale en termes d'architectures.

M. Blancher identifie plusieurs causes à ces phénomènes : On ajoute à l'existant (ajout de couches sur couches). On raisonne en termes de produits, avant de penser à la résilience et à la sécurité de conception des offres proposées.

La seconde tendance en matière de complexité dans l'industrie concerne le personnel technique. Nous avons abouti à une situation où le savoir technique est scindé en deux populations : celle du personnel technique (IT & sécurité), et celle, différente, des décideurs qui planifient l'installation des infrastructures. La conséquence est qu'on installe, dans la plupart des industries, des systèmes qui obligent à intégrer des sources des vulnérabilités.

M. Blancher présente ensuite l'étude de cas illustrative des « exploit kits » proliférant dans les installations Java. En 2006, ces premiers « exploits » visent des vulnérabilités Windows. En 2007-2010, ils migrent vers une exploitation des vulnérabilités dans les produits Adobe (Flash et Reader). De 2010 à 2012, ces mêmes techniques migrent vers des failles Java généralisées à tout système portant ces composants, et notamment, les progiciels de gestion de type SAP. Nous avons donc affaire à une vulnérabilité connue, documentée, qui a déjà fait l'objet de corrections et de contre-mesures, mais que l'industrie elle-même continue de faire proliférer dans des applications commerciales.

Comment expliquer une telle production endogène de vulnérabilités critiques ? La première raison réside dans un certain abandon de l'informatique dans les entreprises qui la considèrent comme une fonction support et donc sous-traitée. Les entreprises doivent malgré tout garder un œil sur le travail des sous-traitants. L'entreprise doit garder des compétences en interne, notamment dans un contexte où les les intérêts entre sous-traitants et clients peuvent être très divergents.

L'objectif principal des départements IT est la réduction de coûts année après année. La politique de sécurité s'en trouve induite par les politiques commerciales des fournisseurs, où les autorisations d'activation sont motivées, elles aussi, par des logiques d'économies de coût commerciales. C'est le cas par exemple de l'utilisation de Smart Phones dans la plupart des grandes entreprises.

M. Blancher rebondit ensuite sur l'intervention de M. JP Macintosh, concernant l'intérêt exagéré porté aux doctrines au détriment de politiques empiriques et pragmatiques. Il identifie l'absence d'inclusion de la sécurité informatique dans les axes stratégiques des organisations comme un de ces principaux facteurs. La dissociation entre le savoir technique et le contrôle des politiques d'équipement par une couche « managériale » avec des lacunes techniques trouve souvent sa source dans la délégation, et la relégation, de la stratégie informatique comme activité secondaire et non critique.

Pour M. Blancher, il est certain que l'Etat a un rôle essentiel à jouer. En reprenant l'exemple donné par M. Molliner, M. Blancher rappelle que la sécurité « active » dans les véhicules a été motivée par une réglementation plus contraignante pour le secteur automobile, avec de réelles sanctions à la clé (Ford et ses feux de freins « incendiaires »). Dans le monde de l'informatique, l'Etat ne joue pas toujours son rôle de régulateur et de protecteur. Les lois aujourd'hui empêchent la formation et le reverse engineering (pour obtenir les codes source dont on ne dispose pas), mais n'étend pas le champ des responsabilités à la sécurité active décrite par les différents intervenants.

Les dispositifs légaux existent, notamment en France, mais leur application rencontre souvent des obstacles d'ordre politique. Par exemple, la CNIL et la loi « informatique et liberté » qui ont pour but la protection des données personnelles. Plusieurs grandes entreprises de distribution françaises ont été sanctionnées pour un non-respect des dispositions légales, mais ces avertissements n'ont eu aucune conséquence. Les grands distributeurs concernés ont continué à enfreindre la loi, sans conséquences financières et sans imposition de corrections.

Il faut bien réaliser, avertit M. Blancher, que les capacités offensives ne sont pas le seul apanage des Etats ou des organisations criminelles. « Monsieur tout le monde » devient un opérateur d'infrastructure critique (ADSL). 40 millions de foyers sont connectés au haut débit. Les attaques de DDOS sur les opérateurs peuvent atteindre les 40 gigas/s. M. Blancher présente un cas d'une attaque qui fut déclenchée à la suite d'un défi lancé par deux participants à une groupe de discussion en ligne. Vexé, l'un des participants a eu recours à l'achat de capacités d'attaque (Botnet) qu'il a trouvé en libre accès alors qu'il était en conversation animée avec son interlocuteur.

Pour conclure, M. Blancher invite à revoir la façon dont on gère les systèmes d'information, la façon dont on conçoit leurs architectures, et dont on forme les informaticiens, et ensuite, adopter la régulation aux objectifs que l'on se donne et que l'on peut atteindre.

Philippe Baumard, Professeur, chaire innovation & régulation, Ecole Polytechnique. "A Triangular Evolution: Doctrines / Regulation / Innovation »

Le Professeur Philippe Baumard présente une analyse de l'interaction entre les techniques, les doctrines et la régulation dans le domaine de la cyber-sécurité. L'objectif de sa présentation est de montrer comment, dans les 40 dernières années, ces trois éléments ont progressivement perdus leur articulation et leur entraînement réciproque.

Le Pr. Baumard présente dans un premier temps le triangle que forme ces trois éléments. Dans ce système d'interaction, les doctrines doivent répondre à des ruptures techniques qui ouvrent de nouveaux vecteurs, défont les règles de conduite en place, et en appellent de nouvelles. En retour, les doctrines ont une influence sur l'innovation en favorisant l'institutionnalisation de domaines plutôt que d'autres. L'exemple récent est celui des APTs qui font l'objet d'une attention importante du corps doctrinaire, au détriment sans doute de l'évolution de techniques simples, mais dont la prolifération est tout aussi importante.

Ce même jeu d'interaction a lieu entre les doctrines et la régulation. Ici, ce sont des « visions du monde » qui sont en compétition, et les enjeux sont politiques et économiques. Les points de tension se situent aux frontières géographiques, légales et économiques.

Finalement, la régulation essaye d'anticiper, par le pré cadrage, les ruptures techniques qui peuvent créer des points d'évasion, tandis que l'innovation est parfois motivée par la création de nouveaux espaces de liberté, d'exploration et de croissance.

L'existence d'un équilibre entre ces trois pôles est importante, mais leur articulation (leur entraînement mutuel) est critique. Pour le Pr. Baumard, c'est la détérioration de cet

entraînement mutuel qui crée les nombreuses vulnérabilités dans le domaine de la cyber-sécurité.

Pour soutenir ce point, le Pr. Baumard présente un historique de l'évolution des formes d'attaques, depuis la naissance des activités de « hacking » à la fin des années 1970 à nos jours. Il oppose la téléologie des attaques (leur but ultime) qui peut se ranger soit dans le « beyond reach » (au delà de la simple atteinte), ou à l'opposé, dans l'attaque non dirigée (à téléologie réduite ou inexistante). Les attaques « beyond reach » poursuivent des motifs ultérieurs, c'est-à-dire que l'attaque elle-même, sa prouesse technique, sa sophistication, n'est pas la motivation intrinsèque de l'attaquant. Les attaques « non dirigées » sont quant à elles plus souvent motivées par l'exploit technique ou la démonstration (parfois égocentrique) de capacité technique de l'attaquant.

Sur un second axe de cette matrice 2 x 2, le Pr. Baumard oppose les attaques « spontanées » (ou sans donneur d'ordre – « paymaster »), des attaques préparées et sponsorisées. Cette matrice permet d'identifier une typologie de quatre formes d'attaques génériques :

- Les attaques de défi d'autorité, qui sont spontanées et non dirigées, et qui forment le cœur historique du « hacking », mêlant dès les années 1980 les « sub-cultures » libertaires, les talents techniques individuels, les gangs autonomes, aussi bien que des pionniers de l'industrie (défi technique) – **CLASSE I**
- Les attaques non dirigées et immédiates, mais qui sont sponsorisées, où l'on retrouve la cybercriminalité « à la demande » et le crime organisé pour les méfaits de droit commun (extorsion, cracking, phishing, vols d'identités), dont le développement en tâche d'huile s'est organisé dans les années 2007-2012, avec des reprises en main de la GCO – **CLASSE II**
- Les attaques à motivation politique, sociétale ou « contre-économiques » (spontanées, sans donneur d'ordre, mais avec une portée qui va au delà de l'attaque elle même) – **CLASSE III**
- Les attaques avancées et sponsorisées (« beyond tech » and « beyond claim ») dont les finalités sont l'influence, le contrôle, la déroute ou la défaite des systèmes ou organisations visées – **CLASSE IV**

Le Pr. Baumard présente ensuite les familles d'attaques dans chaque catégorie, et souligne que la Presse s'intéresse à la Classe IV qui est spectaculaire (guerres de l'information, APTs, cyber-war) mais que la véritable dynamique d'innovation, depuis la fondation du hacking, a lieu dans la Classe I, qui est peu prise en compte par les régulateurs, les investisseurs et les auteurs de doctrines.

Le Pr. Baumard présente ensuite une évolution historique des attaques sur la même matrice. Il commence avec les années 1980, qui sont principalement de Classe I (Ian Murphy, Masters of Deception, Rich Skentra, LoD), tout en soulignant que les attaques de Classe II font déjà leur apparition, et cela dès 1982, avec l'attaque de la First National Bank of Chicago ($70 millions de vol).

Pour le Pr. Baumard, la première rupture se situe dans les années 1990, avec la démocratisation des techniques d'attaques (notamment grâce au groupe « Cult of Dead Cow » et 2600, qui démocratisent de la discipline). La valorisation technique, l'esprit cyber-libertaire perdent du terrain, au profit de petits groupes organisés qui affichent des motivations politiques ou sociétales plus structurées. Moins ludiques, et intégrant des

dimensions « beyond tech », elles visent la prise de contrôle. Elles sont également moins égocentrées, tout en restant largement spontanées. Le Pr. Baumard associe ces mouvements à ce que l'on appelle, de façon abusive, le « cyberespace ».

Les années 2000, avec l'avènement de la monétisation et des modèles économiques sur le réseau des réseaux (Internet) sont identifiées comme l'accélérateur de la cybercriminalité contemporaine. Le Pr. Baumard note que les acteurs de Classe I et II (des années 1980 à fin 1990) sont rares à avoir rejoint ces mouvements. Certains se sont retirés des mouvements et des sous-cultures ou des groupes dans lesquels ils étaient engagés. D'autres ont rejoint l'industrie, ou ont rejoint le monde associatif de défense des libertés numériques. Il n'y a pas de rupture technique fondamentale, si bien que leur moindre implication n'est pas motivée par une obsolescence de leur savoir (qui existe et est relative), mais plus par un refus de participation à l'émergence de la Classe III. Les exemples d'Aleph (Aum Shinrikyo, 1994), Vladimir Levin, 1995), l'extorsion organisée russe (2000-2003) sont cités comme illustrations de cette classe III. Le Professeur Baumard situe dans cette même période ce qu'il appelle la « troisième guerre froide » avec le début des confrontations cybernétiques entre Etats (la campagne de « defacing » de 2001 entre Chine et Etats-Unis), Titan Rain en 2003, etc).

Finalement, Le Pr. Baumard décrit la période 2005-2012, où il note deux phénomènes en forte expansion. La transformation des attaques étatiques de la classe III à la classe IV. Les attaques de contrôle ont des finalités qui dépassent la déstabilisation immédiate et sont des parties de campagnes plus larges (Night Dragon, 2009 ; Stuxnet, 2009, 2007, Estonia, etc.). Les motivations de ces attaques ne sont pas les systèmes visés, mais entrent dans des cadres de négociation plus larges (disputes territoriales, accords commerciaux, conflits du Moyen – Orient, spéculations financières). Parallèlement, les mouvements spontanés, cyber-libertaires, et ultra-individualistes, bénéficient du « crowd sourcing » et de la grande disponibilité de vecteurs d'attaques en libre accès pour le public. C'est la naissance des « groupes » (qui n'en sont pas réellement) comme Anonymous, ou interchangeabilité des représentants, ambiguïtés causales, causes sincères et nobles, et causes futiles (ex : attaque sur le métro de San Francisco – le BART – pour réclamer un meilleur Wifi dans les trames).

Le Pr. Baumard utilise ensuite ce même historique pour créer quatre familles de doctrines :

- **Les doctrines de l'ordre social** (en réponse aux Classes I). Obsolètes, en retard sur la société, elles visent à créer des murs verticaux et juridictionnels par le contrôle direct et la censure. Elles sont dominées par une expertise sécuritaire, avec des visions nationales faibles ou empruntées.
- **Les doctrines technocrates** (en réponse à la Classe II). Ce sont les doctrines des « derniers entrants » dans le champ de la cyber-sécurité. Elles sont défensives et témoignent de l'incompréhension technique des décideurs. La philosophie est celle de la réponse à l'incident, nourrie par une perception technocratique et en décalage avec l'état de l'art. Elles incluent un volet offensif, qui déborde souvent sur la dépravation des libertés individuelles.
- **Les doctrines de résilience sociétale** (pour répondre à la Classe III). Elles sont ancrées dans une vision sociétale, et sont souvent produites par des Etats dont la sensibilité à l'opinion publique est forte. Elles essayent d'utiliser l'espace public comme levier (politiques nationales de soutien aux études de cyber-sécurité) et possèdent un volet « guerre de l'information » actif.

- **Les doctrines de cyber-souveraineté** (en réponse à la Classe IV). Elles associent la maîtrise des capacités cybernétiques à un axe de puissance et de souveraineté. Ces Etats ont développé assez tôt des corps spécialisés dans la cyber-défense, sont obnubilés par les infrastructures critiques (au détriment de la dimension sociétale), et n'ont pas de tabou concernant la dimension offensive.

Le Pr. Baumard présente et commente ensuite le positionnement de 37 doctrines nationales sur cette matrice. Les documents utilisés sont les publications des Etats concernés sur leurs propres doctrines, des articles de recherche, et des publications émanant d'instituts de défense nationaux (données publiques). Le Pr. Baumard en a fait trois grandes « familles ». La première, « le pack » est celle des nations ayant affiché une volonté de leadership dans le domaine (Russie, Chine, Israël, Allemagne, Etats-Unis). Leurs visions favorisent la coordination entre agences, et intègrent des lignes de cyber-défense couvrant des juridictions civiles et militaires. Une seconde famille est celle que le Pr. Baumard appelle « les cybers », qui ont opté pour un déploiement émergent, ancré dans une transformation sociétale (Japon, Singapour, Finlande, Norvège, Corée du Sud). Les réflexions sur une stratégie numérique nationale ont précédé les réflexions sur les stratégies de cyber-sécurité (parfois pour des motifs géographiques comme l'éloignement). Une troisième famille est celle des « explorateurs », partagés entre des doctrines d'ordre social numérique et des doctrines technocrates. Beaucoup sont des « Etats suiveurs », ou des Etats qui se sont alignés sur les doctrines de leurs fournisseurs (fournisseurs qui peuvent être les Etats-Unis, la Chine, la Russie, par exemple). Leur réflexion est encore juridictionnelle, avec une priorité donnée à la défense des infrastructures techniques.

Pour conclure, le Pr. Baumard présente quatre futures formes d'attaques encore mal couvertes par les doctrines existantes : les attaques d'automation (visant les interactions machine-à-machine), les attaques de résilience (visant la spéculation sur les matières premières ou les supports de vie), et les attaques « causatives » (visant les mécanismes de décision et les systèmes d'apprentissage, notamment dans le secteur financier), et les « guerres de discrétion » qui, à l'opposé des guerres d'opinion, visent à soustraire de l'espace public ou des systèmes de contrôle des cibles ou des activités (illicites).

Le diagnostic présenté par le Pr. Baumard rejoint celui des intervenants de la journée. Sur la période 1990-2012, il existe peu de ruptures technologiques, et les vecteurs d'attaques sont stables (technologies élémentaires). Le résultat est une désarticulation profonde entre des infrastructures vieillissantes et des doctrines qui prolifèrent sur des visions techniques qui ont vingt ans de retard sur l'état de la société.

Speakers Bios:

Dr. JP Macintosh
University College, London

Institute for Security and Resilience Studies

After a decade's service with the British Army, Dr MacIntosh left to become a research scientist at the Ministry of Defence. His research focuses on the capacity for decisive action and learning beset by the uncertain flow of events, particularly in evolving networks. This research has also enabled him to fulfill several advisory roles for Cabinet Ministers and senior decision-takers, in the UK and abroad. Commissioned by the then Cabinet Secretary – now Lord Wilson of Dinton – Dr MacIntosh co-authored the concept of "Resilience to Crises" for the UK Government in spring 2001.

Before joining the Institute, he was the Chief of Research and Assessment at the Defence Academy of the UK (where he also served on the Board for three years). In addition to working with defence departments, Dr MacIntosh has also worked with foreign, finance, interior and justice ministries and national crisis management centres in many countries. He has built teams that have worked in operational theatres and with many organisations facing the challenge of deep transformation – in and out of conflict. How strategies gain traction through innovation remains core to his work as ISRS Director of Programmes.

Dr. Chris Demchak
Professor
Strategic Research

Dr Chris C. Demchak, a research professor, a cochair of a group studying cyber conflict, and author of book *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (2011 UGA Press), and of a number of other articles on security, surprise, large complex socio-technical systems, and the evolution of cyberspace holds two masters degrees, respectively, in economic development (Princeton) and energy engineering (Berkeley). She has published numerous articles on societal security difficulties with large-scale information systems to include cybered conflict, national cyber power, and cyber privacy ("theory of action", "BIK behavior-based privacy"), security institutions (CT "Knowledge Nexus") and new military models ("Atrium model" for joint forces).

As co-Director of the new Naval War College Center for Cyber Conflict Studies (C3S), Demchak's research will continue to focus on the evolution in socio-technical systems, surprise in organizations, cyber tools, social integrations, and range of choices emerging in westernized nations' cybersecurity/deterrence strategies. Her emphasis remains on comparative operational institutional learning, advanced use of tools and cognition, and system-wide resilience against normal or adversary imposed surprise.

Arnaud Coustillière
Rear-Admiral,
Officer General for Cyber-Defense, EMA

Rear-Admiral Arnaud Coustillière is the Officer General for Cyber-Defense for the French Chief of Staff, Director of the general coordination for the Ministry of Defense on cyber-defense domain. Rear-Admiral Coustillière's mission includes the definition of the military cyber-defense policy, the plans of action to improve the military cyber-defense strategy, and to conduct cyber defense mission. Rear-Admiral Coustillière spends most of his career as commanding officer or operational officer at sea, before joining in 2008 the Joint Staff as capability manager for telecommunications and cyber-defense.

In 2012, Rear-Admiral Coustilliere presented a first plan for building a "cyber-defense" reserve force, based on volunteers, civil and reserve military officers with advanced skill in cybersecurity. He is currently the Head of the cyber-defense operational command that includes the military emergency responses cell.

Cédric Blancher

Cédric Blancher, Eng. (ENST), is Senior Expert, Cyber-Security for the EADS

Senior Cyber-security Expert, EADS

Group. After a career in consulting in cyber-security, he joined EADS in the newly created cyber-security laboratory of Innovation Works, becoming the Director of the Cyber-security Lab in 2006. A contributor to leading cyber-security publications, and a participant to the French chapter of the Honeynet Project, Mr. Blancher has been a visting researcher with the UC Berkeley TRUST center, and is an associate professor at ESIEA.

A member of the "Contemporary Threats, Information Technology and New Criminality" Committee of the Scientific Council of the French High Council for Strategic Research (CSFRS), Mr. Blancher led the Council's White Report recommendations on cyber-security policy. His wide breath of expertise includes network defense, embarked systems security, security protocols, and transmissions. A promoter of open source, Mr. Blancher is also a participant in NGOs helping the development of software skills in emerging countries.

John Mallery
Research Scientist
MIT - CSAI Lab

John C. Mallery is a research affiliate at the MIT Computer Science & Artificial Intelligence Laboratory. His recent research involves national cyber strategy, escalatory models of cyber conflict, architectures for international cyber sharing and collaborative analysis, threat reduction via cyber norms, and technical strategies for cyber defense. He is generally concerned with cyber policy and has been developing advanced architectural concepts for cyber security and transformational computing for the past decade.

During the 2008 Presidential campaign, he served on Obama's cyber policy team and helped craft his July 16, 2008 cyber platform. Since 2006, he organized a series of national workshops on technical and policy aspects of cyber. His interests span a variety of fields from artificial intelligence, computer science and information assurance to cyber defense, economics and international relations.

Jean-Luc Moliner
Senior Vice President
Cyber-Security, Orange

Jean Luc Moliner is since may 2011, Senior Vice President, Head of France telecom Group Security in charge of the global security in FT footprint (35 countries and the Business lines) with a strong focus on IT&N security. Before he spent 6 years in the Defense & security division of the EADS company, as VP Sales & Marketing winning the worldwide leadership in the Homeland security market with focus in Middle East.

Previously he worked in the French MoD as Head of Information Systems Security for the Joint Staff, Head of SIGINT division in the French Intelligence Service, Head of the Key Distribution National Agency, Regiment Commander in Germany and in several staff and forces positions. He graduated from the Ecole Spéciale Militaire de Saint Cyr, Ecole Nationale Supérieure des télécommunications & from the french War College.

Philippe Baumard
Professor, Ecole Polytechnique, Chaire Innovation & Regulation

Dr. Philippe Baumard is Professor of Strategic Management at the University Paul Cézanne Aix Marseille, and Researcher of Ecole Polytechnique Chaire Innovation and Regulation of Numerical Services. Dr. Baumard was elected President of the Scientific Council of the High Council for Education and Strategic Research (CSFRS) in March 2010.

Professor Baumard's recent books include *Le vide stratégique* (CNRS Editions, 2012), *International Financial Sanctions* (Ed., 2012), and the direction of the national White Paper on strategic research published by CSFRS (Ed., *Questions de future*, 2012). A panel member of the Innovation & Organizational Sciences division of the National Science Foundation, Dr. Baumard also served as Corporate Strategy Advisor for France Telecom Group, from 2000 to 2004, prior to joining the Berkeley High Reliability Organizations team at the Center for Catastrophic Risk Management. A fellow of the Oxford-Sorbonne Chancellors grant, Dr. Baumard has been a visiting faculty member at New York University, Lund University (Sweden), University of Technology, Sydney, University of California, Berkeley, and Stanford University.