Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
**Ambassade de France au Japon**
**Service pour la Science et la Technologie**

Rapport d'Ambassade

# La cybersécurité au Japon & coopération scientifique franco-japonaise

Octobre 2016

Rédacteur :

## Yan-Tarō Clochard

Chargé de mission, Sciences et Technologies de l'Information et de la Communication (STIC)

Service pour la Science et la Technologie (SST)

Relecteur :

## Evelyne Etchebéhère

Attachée, Sciences et Technologies de l'Information et de la Communication (STIC)

Service pour la Science et la Technologie (SST)

# Résumé :

***La cybersécurité, enjeu majeur au Japon et en France***

L'essor des sciences et technologies de l'information et l'extension du réseau internet aux objets communicants constituent de formidables opportunités tout en rendant nos sociétés de plus en plus vulnérables aux risques inhérents au cyberespace. Les cyberattaques contre les institutions gouvernementales, les infrastructures stratégiques, les entreprises et les individus se sont considérablement développées et sophistiquées au cours des dernières années. La cybersécurité est désormais un enjeu de respect de la vie privée, de compétitivité et de souveraineté nationale. Savoir anticiper, créer la confiance, protéger les données et gérer les crises est aujourd'hui essentiel.

Ce sujet est une problématique d'intérêt commun entre la France et le Japon. D'une part, en France, il a été identifié comme un enjeu de sécurité nationale dans le cadre du Livre blanc sur la défense et la sécurité nationale en 2013 et un thème clé pour la compétitivité industrielle française, faisant l'objet de l'un des 34 plans de la Nouvelle France Industrielle, et a fait l'objet d'un document stratégique spécifique fin 2015 (stratégie nationale pour la sécurité du numérique). D'autre part, le gouvernement japonais a inscrit ce domaine comme l'un de ses axes nationaux prioritaires comme en témoignent la stratégie de cybersécurité japonaise initialement publiée en juin 2013 et revue en 2015 et le *Basic Act on Cybersecurity* adopté au Japon en novembre 2014. Par ailleurs, la tenue des jeux olympiques en 2020 à Tokyo fera du Japon une cible privilégiée de cyberattaques. Conscient de cette menace, le pays va investir fortement dans les solutions technologiques pour assurer sa résilience face à ses attaques.

Dans un cyberespace de plus en plus incertain il est crucial de renforcer les relations avec nos partenaires internationaux de confiance. La France et le Japon, qui partagent un certain nombre de valeurs communes : libre circulation de l'information, liberté d'expression, mais également un grand nombre de cybermenaces similaires ont tout intérêt à développer leur coopération. La France et le Japon ont lancé en 2014 un dialogue politique bilatéral afin de joindre leurs efforts sur ce sujet, dont la prochaine édition devrait avoir lieu en début d'année 2017 à Paris.

Afin d'alimenter ce dialogue d'un point de vue scientifique et technologique, une initiative a été en place entre la France et le Japon suite à un événement organisé par l'ambassade de France au Japon. Cette initiative, qui s'inscrit sur le long terme et fait preuve d'un fort dynamisme, permettra aux deux pays de joindre leurs forces, tout en préservant leur souveraineté nationale dans ce domaine.

# Table des matières

# Introduction

Les cyberattaques se multiplient dans le monde entier, causant des préjudices colossaux aux gouvernements, aux sociétés privées et bien évidemment aux citoyens (détournements de fonds, usurpations d'identité, chantages, mise en danger de l'organisation des entreprises et atteinte à leur image, etc.).

Les données et systèmes sont ciblés par des agresseurs variés, visant à récupérer des fichiers clients, des données personnelles des utilisateurs, salariés, dirigeants, actionnaires, des informations financières, des éléments de propriété industrielle, secret médical, des emails, etc. Les dommages et dangers peuvent également être majeurs lorsque les cibles correspondant à des « infrastructures critiques » (ex : énergie, finance, transport, santé…).

Dans notre société dont la connectivité ne cesse d'augmenter, ces menaces deviennent omniprésentes et globales. Les attaques ciblent désormais les grands groupes comme les PME (les attaques ont augmenté globalement de 42 %, mais elles ont plus que doublé pour les entreprises de moins de 250 salariés), les gouvernements comme les individus dans divers buts. Les attaquants peuvent avoir des motivations très différentes : revendications politiques, intérêt lucratif, volonté de détériorer l'image d'une marque... D'après Trend Micro, le Japon était en 2014 la première victime de logiciels malveillants visant le système bancaire[1] après les Etats-Unis[2].

Une des difficultés majeures rencontrées par les gouvernements est la non-divulgation par les entreprises, par crainte d'impact sur leur image, des problèmes rencontrés et des attaques subies.
Dans ces conditions, l'estimation de l'impact financier de telles actions sur l'économie est donc difficile à estimer. L'impact des cyberattaques dans le monde serait ainsi compris entre 100 et 300 milliards d'euros.

La cybersécurité a été identifiée comme un axe particulier d'effort dans la Stratégie de sécurité nationale japonaise publiée pour la première fois en décembre 2014. Le Japon s'attache en effet depuis quelques années à combler son retard en matière de capacités techniques, avec l'appui de l'allié américain, en vue de développer un système national robuste contre les cyberattaques et d'améliorer la coordination au sein du gouvernement, ainsi qu'avec le secteur privé et académique.

De manière plus récente, l'accent est également porté sur la coopération internationale. Le Japon est en effet désireux d'accroître ses réseaux d'échanges d'information, de mieux coordonner en amont ses positions dans les enceintes internationales pertinentes et de développer une offre d'assistance dans des zones économiquement et politiquement stratégiques pour lui (Asie du sud-est et Afrique).

Enfin d'après la Commission Européenne, le marché mondial de la cybersécurité était d'environ 60 milliards d'euros en 2013 (dont 17% en Europe) et devrait atteindre 90 milliards d'euros dès 2018[3] (estimé à 4 milliards d'euros en France avec une croissance annuelle d'environ 10 %). La cybersécurité constitue donc également une formidable opportunité de développement économique.

---

[1] http://www.trendmicro.es/media/wp/wp-the-japanese-underground-en.pdf

[2] http://www.trendmicro.es/media/wp/wp-the-japanese-underground-en.pdf

[3] Voir CybersecurityPublic-PrivatePartnershipInfographic

# I. Stratégie et acteurs de la cybersécurité en France

## 1. Stratégie française en cybersécurité

### a. La France, acteur majeur de la stratégie européenne

L'Union Européenne s'est dotée en 2013 d'une stratégie sur la cybersécurité, pour préserver un internet ouvert et garantir la liberté et les opportunités en ligne[4].

En juin 2016, la Commission Européenne a annoncé un ensemble d'initiatives pour mieux préparer l'Europe contre les cyberattaques et renforcer la compétitivité du secteur de la cybersécurité, notamment, dans le cadre notamment de sa stratégie pour le marché unique numérique :

- Le lancement d'un **partenariat public-privé européen sur la cybersécurité** (réunissant acteurs de l'administration, entreprises, universités et centres de recherche), qui devrait générer 1,8 milliard d'euros d'investissements d'ici à 2020. L'UE investira 450 millions d'euros via son programme pour la recherche et l'innovation Horizon 2020, tandis que les acteurs industriels représentés par l'organisation européenne pour la cybersécurité (ECSO), devraient investir jusqu'à 1,3 milliard d'euros.
- La **directive sur la sécurité des réseaux et de l'information** (NIS), qui vise à augmenter les capacités des pays membres à lutter contre les cybermenaces et la coopération transfrontalière, à travers :
    - Le renforcement des capacités nationales de cybersécurité de chaque état
    - Le développement de la coopération entre états membres de l'UE en matière de cybersécurité, sur une base volontaire, sur les aspects politiques et opérationnels de la cybersécurité
    - Le renforcement par chaque état de la cybersécurité de ses « opérateurs de services essentiels » via la mise en place d'un cadre de protection
    - l'instauration de règles européennes communes en matière de cybersécurité pour les prestataires de services numériques

Le programme pour la **recherche et l'innovation Horizon 2020** (2014-2020)consacre déjà des financements pour la recherche en cybersécurité dans ses premiers appels.

Sur la période 2016-17, plusieurs appels sont dédiés à la cybersécurité, dans le volet concernant la sécurité des sociétés européennes[5], plus particulièrement :

[4] http://europa.eu/rapid/press-release_IP-13-94_en.htm

[5] 14. Secure societies – Protecting freedom and security of Europe and its citizens : http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

- Protection des infrastructures critiques
  - CIP-01-2016-2017
- Call – Sécurité numérique
  - DS-01-2016: Assurance et certification de systèmes ICT, services et composants fiables et sécurisés
  - DS-02-2016: Cybersécurité pour les PMEs, administrations publiques locales et individus
  - DS-03-2016: Améliorer la sécurité numérique pour les données de santé, à un niveau systémique
  - DS-04-2016: Economie de la cybersécurité
  - DS-05-2016: Coopération dans le cadre de l'UE, Dialogues internationaux dans le domaine de la cybersécurité, recherche et innovation pour la confidentialité des données
  - DS-06-2017: PPP sur la cybersécurité: cryptographie
  - DS-07-2017: PPP sur la cybersécurité: Faire face aux menaces cyber avancées et à leurs auteurs
  - DS-08-2017: PPP sur la cybersécurité: confidentialité, protection des données, et identités numériques

Concernant la dimension internationale de ces appels (DS-052016), la Commission Européenne a identifié le Japon et les Etats-Unis comme pays cibles pour la coopération, qui sera développée au travers de la mise en place d'Actions de Soutien et de Coordination (C.S.A.).

### b. Stratégie de cybersécurité nationale en France

Les prémices de la stratégie de cybersécurité nationale ont été énoncées dans le « Livre blanc sur la défense et la sécurité nationale » en 2008. En 2009, l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI)a été créée par le gouvernement et placée sous l'autorité du SGDSN (Secrétariat général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre). L'ANSSI assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information.

En Octobre 2015, la France annonce sa « **stratégie nationale pour la sécurité du numérique** », organisée autour de 5 objectifs :

- Se donner les moyens de défendre ses intérêts fondamentaux dans le cyberespace, en consolidant la sécurité numérique des infrastructures critiques et œuvrer pour celle des opérateurs essentiels à l'économie.

- Développer un usage du cyberespace conforme à ses valeurs et y protéger la vie numérique des citoyens, en renforçant la lutte contre la cybercriminalité et l'assistance aux victimes d'actes de cybermalveillance.
- Sensibiliser dès l'école à la sécurité du numérique et aux comportements responsables dans le cyberespace. Les formations initiales supérieures et continues intégreront un volet consacré à la sécurité du numérique adapté à la filière considérée.
- Développer un écosystème favorable à la recherche et à l'innovation et faire de la sécurité du numérique un facteur de compétitivité. Il s'agit d'accompagner le développement de l'économie et la promotion internationale des produits et services numériques, mais également de s'assurer de la disponibilité pour les citoyens, entreprises et administrations, de produits et services numériques présentant des niveaux d'ergonomie, de confiance et de sécurité adaptés aux usages et aux cybermenaces.
- Constituer, avec les États membres volontaires, le moteur d'une autonomie stratégique numérique européenne et jouer un rôle actif dans la promotion d'un cyberespace sûr, stable et ouvert.

D'autre part, le Ministère de la Défense a inscrit la cybersécurité comme l'une des priorités de son livre blanc sur la défense et la sécurité nationale[6].

Enfin, la feuille de route du plan cybersécurité (P33)[7] de la nouvelle France industrielle (coordonné par l'ANSSI) fixe les 4 objectifs de la filière :

- Accroître significativement la demande en solutions (produits et services) de cybersécurité de confiance
- Développer pour les besoins de la France des offres de confiance
- Organiser la conquête des marchés à l'étranger
- Renforcer les entreprises nationales du domaine cybersécurité

Il fixe aussi 16 actions structurantes incluant une forte relation avec la R&D, ainsi que la création d'un label « France Cybersecurity » (voir ci-après).

## 2. L'excellence cyber française

### a. L'agence nationale de la sécurité des systèmes d'information (ANSSI)

[6] https://www.ssi.gouv.fr/publication/la-cybersecurite-au-coeur-du-nouveau-livre-blanc-sur-la-defense-et-la-securite-nationale/

[7] https://www.ssi.gouv.fr/uploads/2015/01/Plan_cybersecurite_FR.pdf

L'ANSSI est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. Elle apporte également son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV).

Elle est chargée de la promotion des technologies, produits et services de confiance, des systèmes et des savoir-faire nationaux auprès des experts comme du grand public, notamment par la labellisation de produits et de prestataires. Elle contribue ainsi au développement de la confiance dans les usages du numérique. Son action comprend également le développement de produits et une offre de formation.

L'ANSSI collabore également étroitement avec ses partenaires internationaux pour coordonner l'effort international d'amélioration de la cybersécurité.

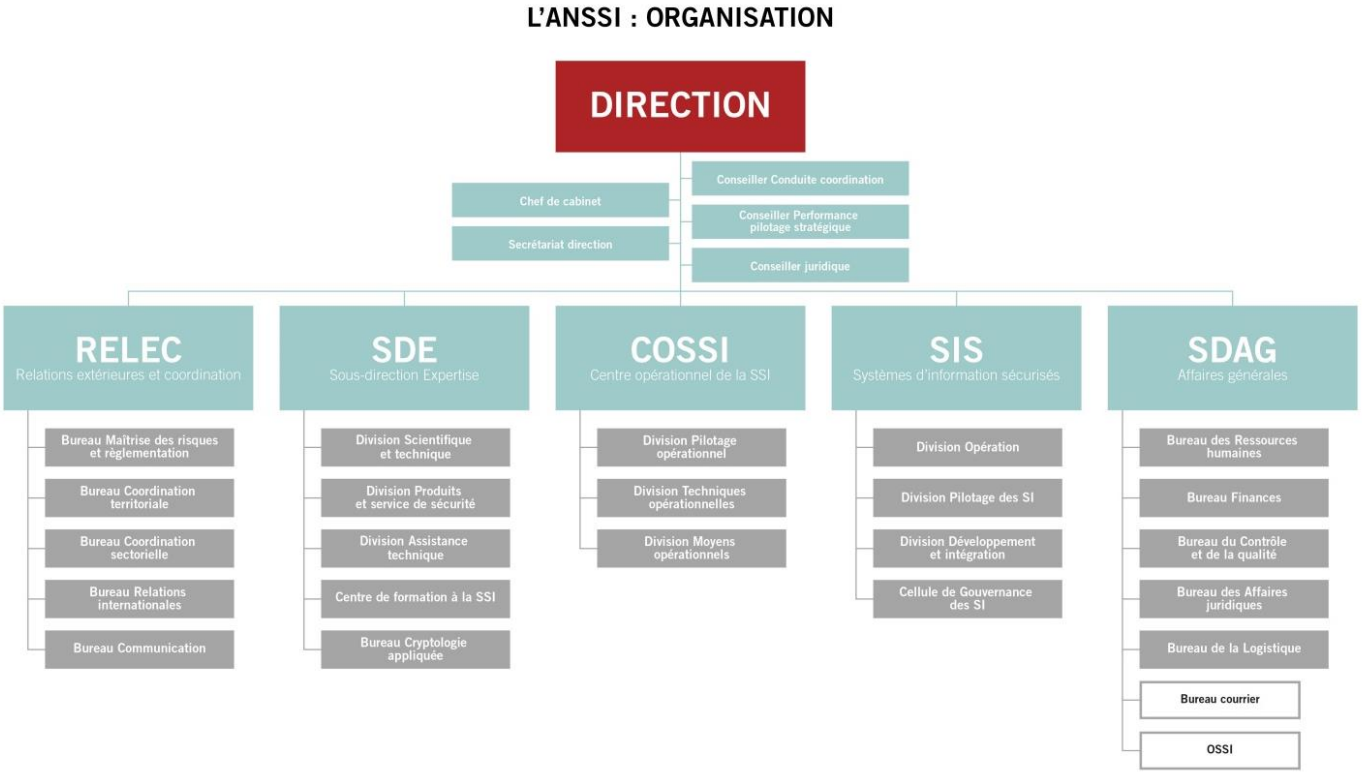



Figure 1 : Organigramme de l'ANSSI

## b. Les acteurs de la cybersécurité en France, panorama général

**Réseau Hexatrust**

Le réseau Hexatrust, lié à l'ANSSI, regroupe des PME, ETI, industriels du logiciel français en sécurité des systèmes d'information et cybersécurité, certifiées par l'ANSSI8.

Hexatrust s'est associé en octobre dernier au Groupement des industries françaises de défense et sécurité terrestres et aéroterrestres, qui s'est doté d'une direction des systèmes d'information. A noter que déjà en 2008, le Livre blanc sur la défense et la sécurité nationale plaçait la sécurité des systèmes d'information au même rang que la dissuasion nucléaire et le secteur des missiles balistiques ! Le groupement travaille avec l'Agence nationale de sécurité des systèmes d'information, à la mise en œuvre du Plan 33 « Cybersécurité » de la Nouvelle France industrielle, qui envisage notamment la création d'un « label France », une marque de confiance, de qualité et de performance pour les offres nationales.
Hexatrust regroupe un large éventail de technologies : pare-feu, antivirus, systèmes de veille, de détection des intrusions, de protection contre les intrusions, services de cloud, etc. Les membres d'Hexatrust réalisent à l'international 39 % du volume de leurs ventes, pour un chiffre d'affaires global de 110, 4 millions d'euros en 2014, en progression de 17,5 %.

Les industriels du secteur de la confiance et de la sécurité ont décidé de se structurer en créant le CICS (Conseil des industries de confiance et de sécurité). Le CICS a été constitué par quatre syndicats professionnels – FIEEC, GICAN, GICAT et GIFAS – tous fortement impliqués dans les équipements et solutions de sécurité[9].

Enfin, Hexatrust et GICAT (Groupement des Industries françaises de défense et sécurité terrestres et aéroterrestres) ont également décidé de s'allier pour promouvoir la filière de la cybersécurité française à l'export[10].

Le comité de la filière industrielle de sécurité (CoFIS, mis en place par le Premier ministre en octobre 2013) a lui pour objectif de fédérer les efforts de l'État, des collectivités territoriales, de l'industrie, de la recherche et des grands opérateurs publics et privés, pour développer des solutions de sécurité de meilleure qualité et exportables à l'étranger.

**<u>Un tissu industriel fort et un grand nombre de PME innovantes</u>**

Sur ce marché on trouve évidemment d'importants groupes industriels, tels que Thalès, Airbus Group, Atos-Bull, Safran, Gemalto, Oberthur Technologies mais aussi de nombreuses entreprises de taille plus modeste.

[8] http://www.lemagit.fr/actualites/2240206444/Hexatrust-le-club-de-la-securite-made-in-France

[9] https://www.cics-org.fr/

[10] http://www.industrie-mag.com/article5092.html

Parmi les championnes tricolores, Dictao, spécialiste de la sécurisation des transactions (authentification, coffre-fort numérique…), très présente dans l'administration, la banque, l'assurance, a ouvert des filiales en Espagne, au Danemark et s'implante au Royaume-Uni.

Une autre caractéristique notable du paysage français est ainsi l'émergence d'un fort tissu de PME innovantes dans le domaine de la cybersécurité au sens large. On peut par exemple citer : Vade Retro, Olfeo, Wallix, Opentrust, DenyAll, Ilex, Netheos, Sistech, InWebo, Brainwave, Arismore, Bertin Technologies ou Secure-IC[11].

**Le Label France Cybersecurity[12]**

Le Label France Cybersecurity, mis en place suite au plan pour la cybersécurité pour la Nouvelle France industrielle, a pour but de garantir à l'export et pour les marchés publics une qualité et des savoir-faire reconnus. Il est animé par :

- une structure de gouvernance composé des parties prenantes de la cybersécurité, réunis en trois collèges : étatique (Direction générale de l'armement (DGA), de la Direction générale des entreprises (DGE) du Ministère de l'économie, de l'industrie et du numérique et de l'ANSSI), industriel (représentants de l'Alliance pour la Confiance Numérique (ACN) et d'Hexatrust) et utilisateur (CIGREF, GITSIS, CESIN)
- une structure d'attribution du label.

Liste des sociétés listées :
http://www.francecybersecurity.fr/wp-content/uploads/2016/08/FCS_Catalogue_2016_web.pdf

**Le Pôle d'Excellence Cyber Bretagne (PEC)**

Le Conseil régional de Bretagne et le ministère de la Défense ont initié en février 2014 le Pôle d'excellence cyber Bretagne (PEC). Ce pôle, de portée nationale et à rayonnement international, vise à fédérer et structurer l'ensemble des acteurs de la recherche, de la formation et du développement économique avec pour objectifs :

- d'optimiser l'utilisation des moyens et le développement des compétences cyber du ministère présents en Bretagne en y concentrant les unités ;
- de stimuler la recherche, la formation et l'innovation en s'appuyant sur un tissu académique et industriel dense et favoriser le développement de la filière industrielle, y compris à l'export ;
- de créer un cursus de formation à la conduite des opérations et à la gestion des crises cyber et à la cyberdéfense qui sera ouvert aux partenaires publics ou étrangers ;

[11] http://www.ambafrance-jp.org/Les-entreprises-francaises-a-la

[12] http://www.francecybersecurity.fr/

Le pôle regroupe plus de 120 entreprises de toutes tailles spécialisées dans la cybersécurité, 13 équipes de recherche académique, 200 chercheurs travaillant sur cette thématique, une offre de formation, la présence de l'expert technique du Ministère de la Défense (DGA Maîtrise de l'information à Rennes), de centres de formation militaire d'excellence (Saint-Cyr Coëtquidan, École navale, École des transmissions...), et la présence de grands groupes tels que Thales, DCNS, Orange, Nokia.


Figure 2 : Les acteurs de la cybersécurité en Bretagne[13]

Orange cyberdéfense a également affiché son intention de créer un Pôle d'Excellence cyber à Lille dans les années à venir[14].

## 3. Stratégie de recherche sur la cybersécurité en France

### a. Organisation de la recherche publique en France

A l'échelle nationale : l'Agence Nationale de la Recherche (ANR) soutient fortement la cybersécurité à la fois comme thème de recherche principal et ses applications :

[13] http://www.bretagne.bzh/upload/docs/application/pdf/2016-01/pec_n8_carte_bzh_2300x2500mm_1ex.pdf

[14] http://www.industrie-techno.com/fic-2016-orange-va-creer-a-lille-un-nouveau-pole-d-excellence-en-cybersecurite.42279

- Challenge 7 : société de l'information et de la communication
- Challenge 9 : Liberté et la sécurité de l'Europe, de ses citoyens et de ses résidents.

L'agence a financé plusieurs projet dans le domaine cyber, dont :

- AJACS : Applica4ons JavaScript : Analyses Certifiées et Sécurité
- BRUTUST : Chiffrements authentifiés et résistants aux attaques par canaux auxiliaires
- EnBiD : Chiffrement des masses de données
- ADAX : Attack Detection And Countermeasures Simulation

Les principales institutions de recherche française (centres de recherche, universités) ont largement identifié la cybersécurité comme étant un thème de travail majeur à développer.

Par exemple, l'année 2016 a ainsi été proclamée « année de la sécurité » à l'INS2I (Institut des sciences informatiques et de leurs interactions) du CNRS.

L'alliance Allistene (l'alliance des sciences et technologies du numérique, ayant pour objectif notamment la coordination entre les acteurs de la recherche française entre le CDEFI, le CEA, le CNRS, la CPU, Inria, l'Institut Mines-Télécom, etc.) s'est notamment doté d'un groupe « Cybersécurité »[15] ayant pour objectifs:

- pilotage de l'action 7 de la feuille de route cybersécurité : « Mieux piloter la R&D en cybersécurité et accroître sa valorisation »;
- action de veille en matière de cybersécurité et développement d'une stratégie d'influence;
- coordination avec le programme « H2020 ».

L'animation du groupe est confiée à Jean Mairesse (CNRS) et à Claude Kirchner (Inria), sous le pilotage de Michel Bidoit (CNRS)[16].

Une des premières tâches de ce groupe de travail sera de cartographier les axes de travail des organismes de recherche nationaux.

Un projet de groupement de recherche (GDR[17]) au niveau national sur la cybersécurité est également initié, sous l'impulsion de Gildas Avoine de l'INSA de Rennes : le pré-GDR Sécurité Informatique[18].
Il portera sur les thématiques suivantes[19] :

- Codage et cryptographie (commun avec GDR IM)
- Protection des données personnelles
- Sécurité et données multimédia (commun avec GDR Isis)
- Sécurité des réseaux et des infrastructures
- Sécurité des systèmes logiciels
- Sécurité des systèmes matériels (commun avec GDR SoC-SiP)

[15] https://project.inria.fr/allistene/files/2016/03/presentationAllistene-2016-03-17-GTCybersecurite.pdf

[16] https://www.allistene.fr/organisation-allistene/groupes/groupe-cybersecurite/

[17] http://www.cnrs.fr/inshs/recherche/actions-propres-institut/gdr/gdr.htm

[18] http://gdr-securite.irisa.fr/

[19] http://gdr-securite.irisa.fr/download/presentation_gdr_avoine.pdf

Le préGDR organise d'ores et déjà plusieurs événements : l'école d'été "Cyber in Bretagne"[20], organisée conjointement avec le Pôle d'Excellence Cyber (la première édition a eu lieu du 4 au 8 juillet 2016), ainsi qu'une semaine de rencontres entre entreprises et doctorants (REDOCS).

La structuration et l'effort français en matière de cybersécurité est conséquent et implique l'ensemble des acteurs du monde institutionnel, académique et privé.

### b. Les principaux acteurs de la recherche et formation en cybersécurité en France

Dans le domaine de la recherche

Les principaux acteurs du monde de recherche en cybersécurité en France sont les plus importants centres de recherche nationaux (CEA, CNRS, Inria, Institut Mines-Telecom) ainsi que certaines Universités et Grandes Ecoles.

Environ 650 personnes du monde académique sont actuellement concentrées sur le sujet en France (incluant les chercheurs permanents, professeurs, étudiants doctorants et post docs).

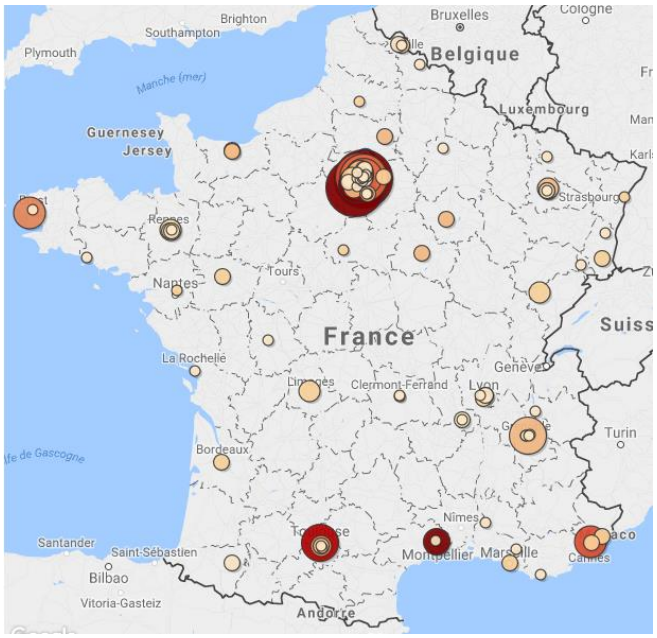



**Figure 3 : localisation des principaux laboratoires travaillant sur la cybersécurité en France (par nombre de publication)**

[20] https://project.inria.fr/cyberinbretagne/fr/

Parmi les institutions de recherche en cyber sécurité, on retrouve les « laboratoires de haute sécurité (LHS) ».

Dans le monde académique, les premiers LHS ont été ouverts à Nancy, Rennes et le troisième sur le campus de Paris-Saclay (en construction).

Un LHS, est divisé en 3 espaces distincts[21] :

- Une salle de travail qui accueille les chercheurs
- Une salle de clusters dotée de trois unités : un télescope virtuel qui recueille des codes malveillants, des traces d'attaques et qui permet l'expérimentation de sondes sur l'Internet, un réseau fermé dit « éprouvette » qui permet de mener des expériences sensibles comme l'analyse de codes malveillants sans risque de contamination de l'ensemble du réseau et une unité de production pour distribuer les outils développés au sein du LHS : anti-virus, outils d'analyses, etc.
- Une salle dite « rouge ». Non connectée au réseau, elle concerne le traitement d'informations et de données très sensibles. Cette salle permet d'accueillir les équipements ou matériels à étudier en toute confidentialité dans le cadre de partenariats avec les industriels.

Quelques laboratoires menant des recherches sur la cybersécurité :

CEA-Tech:

L'expertise du CEA-Tech en micro-électronique et en développement logiciel lui permet de développer des solutions globales sur la cybersécurité, à travers ses différents instituts[22].

- Leti (Grenoble et Marseille) → sécurité embarquée
- List (Saclay) → Logiciel et sécurité des réseaux

CNRS :

Comme illustré par le choix de 2016 comme année de la sécurité à l'INS2I, les équipes du CNRS développent leurs travaux autour de la cybersécurité.

- IRIT (Toulouse) : confidentialité
- XLIM (Limoges): cryptologie, antennes
- VERIMAG (Grenoble) : sécurité des protocoles
- LORIA (Nancy) : e-vote, virus, cryptographie, protocoles, réseaux
- GREY (Caen) : opérations bancaires digitales, biométrie

[21] https://www.inria.fr/centre/nancy/innovation/laboratoire-securite-informatique

[22] http://www.cea.fr/cea-tech/Documents/Offre%20CEA%20Tech%20march%C3%A9/FR/L'offre%20CEA%20Tech%20pour%20la%20cyber%20s%C3%A9curit%C3%A9.pdf

- IRISA (Rennes) : intrusions, détection, cryptographie
- LSV (Cachan) : sécurité des protocoles, e-vote
- PRISM (Versailles-St Quentin en Yvelines) : cryptologie, base de données sécurisées
- DI-ENS (Paris) : cryptologie
- LAAS (Toulouse )
- LIMOS (Clermont-Ferrand)

Inria :

Les laboratoires de l'Inria travaillant dans le domaine de la cybersécurité sont :

- Madyne (Nancy)
- Diana (Sophia-Antipolis)
- Cidre (Rennes)
- Prosecco :
- Carte
- Cassis
- Dice
- Privatics
- Comete

Ils couvrent un large spectre de thèmes relatifs à la cybersécurité :

- La cryptographie
- Les protocoles cryptographiques
- les méthodes formelles et la vérification pour la sécurité
- l'analyse de code, contrôle de flots d'information et défaillances
- la communication sécurisée dans les réseaux et sur les grilles
- la prévention et détection d'intrusions, la virologie
- la sécurisation et protection des données
- l'identification et la protection de l'individu : biométrie, vidéo-surveillance
- le vote numérique
- la sécurité numérique et société : respect de la vie privée, législation

Institut Mines-Telecom

Plusieurs laboratoires à l'IMT

- SEIDO entre EDF R&D et Télécom ParisTech : Internet des Objets et la cybersécurité pour les systèmes électriques
- Secure Compression Lab (IMT, Doremi, Secure-IC) : compression et de la sécurisation des flux médias
- SERES (Sécurité des Réseaux et des Systèmes d'Information) de Télécom Bretagne
- …

mènent des actions de recherche dans le domaine cyber, essentiellement sur [23]:

- la sécurité des composants : amélioration des pare-feux, nouveaux outils de chiffrement ou développement de nouveaux contrôleurs d'accès
- la cyberdéfense : détection d'intrusions et activation de moyens de lutte efficaces
- la cyber-résilience : conception de systèmes pouvant fonctionner en mode dégradé durant ou après une attaque, afin qu'ils continuent d'offrir les services voulus.

Une chaire sur la cybersécurité des infrastructures critiques a été lancée en janvier 2016, portée par Télécom Bretagne, en collaboration avec Télécom ParisTech, Télécom SudParis, la région Bretagne dans le cadre du Pôle d'Excellence Cyber et 8 entreprises : Société Générale, Airbus Defence and Space, Amossys, BNP Paribas, EDF, La Poste, Nokia et Orange.

L'IMT, l'École navale, DCNS et Thales se sont également associés pour créer, avec le soutien de la région Bretagne, une chaire de cyberdéfense des systèmes navals.

Les compétences françaises en matière cyber sont très larges et du meilleur niveau mondial. Les thématiques suivantes gagneraient toutefois à être développées, notamment dans le cadre international :

- Système d'exploitation sécurisé
- « Tracking » des attaquants
- Géostratégie
- Evolution du système légal
- Facteurs humains, incluant la prise de conscience et l'enseignement de l'informatique et de la cybersécurité

Dans le domaine de la formation

L'offre de formation en lien avec la cybersécurité proposée est en fort développement en France.

On trouve certaines formations spécialisées, notamment :

- Saint-Cyr, à travers la chaire Saint-Cyr, Sogeti, Thalès sur la cyberdéfense et cybersécurité
- IMT : Mastère spécialisé Cybersécurité et cyberdéfense à Telecom ParisTech, formation Expert cybersécurité à Telecom SudParis, mastère spécialisé ingénierie de la cybersécurité à Telecom Lille
- Formations universitaires spécialisées
- …

La liste des formations en cybersécurité en France est disponible sur le site de l'ANSSI : https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/

[23] https://blogrecherche.wp.mines-telecom.fr/2016/01/20/cybersecurite-la-recherche-prend-les-devants/

# II. Stratégie et acteurs de la cybersécurité au Japon

## 1. Éléments de contexte

Le cyber environnement japonais est très complexe et se distingue par de nouvelles caractéristiques :

1. Les attaques sont de plus en plus sophistiquées et visent des informations sensibles (type informations confidentielles). Ce type d'attaques ciblées a quintuplé entre 2012 et 2013.
2. Les attaques se multiplient contre les infrastructures critiques (x1,5 en un an).
3. Le périmètre d'attaque augmente avec les changements sociétaux. La multiplication des objets connectés (smartphones, véhicules autonomes, smart meters, etc.) augmentent le nombre de cibles potentielles, dont le niveau de sécurité général n'est pas suffisant.
4. La plupart des attaques viennent de l'étranger, ce qui pose des problèmes pour le suivi des incidents et les conséquences légales d'attaques.

Les récents exemples d'attaques vers les informations sensibles concernent aussi bien les entreprises que les organisations gouvernementales.
Ainsi Mitsubishi Heavy industries, l'organisation japonaise de sureté de l'énergie nucléaire (JNES), le Ministère de l'agriculture, des forêts et de la pêche, l'agence exploration aérospatiale japonaise (JAXA) ou encore l'agence japonaise de l'énergie atomique (JAEA) ont tous été victimes d'attaques ces trois dernières années.
Les attaques sont variées et difficiles à détecter (infections par un virus, accès non autorisés à des serveurs, etc). Ces attaques sont les plus médiatiques mais chaque jour, les autorités japonaises font face à un nombre croissant d'attaques (en moyenne une toutes les dix minutes).

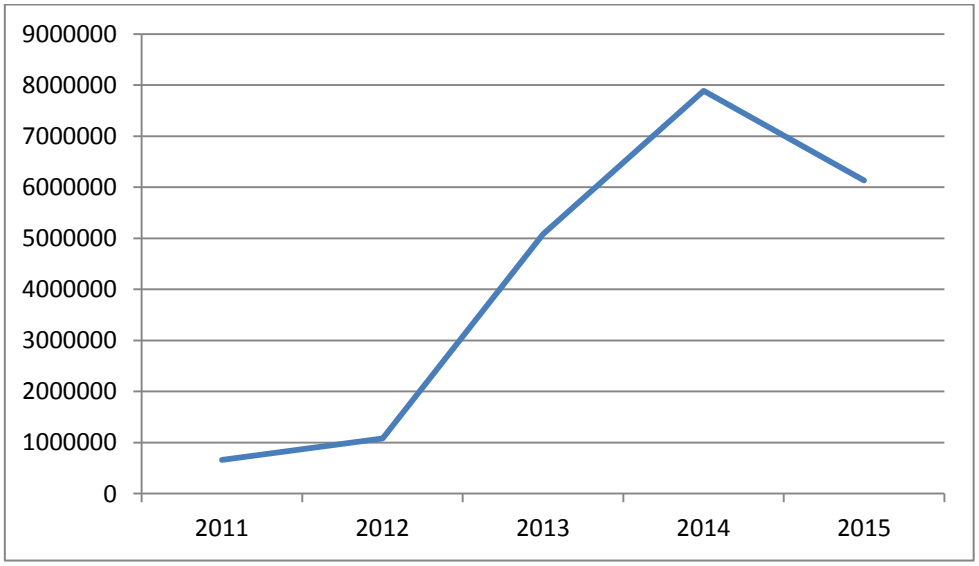



**Figure 4 : Nombre de menaces détectées à travers la surveillance par des capteurs des équipes du GSOC (Government Security Operation Coordination) japonais**

Attaques sur les infrastructures critiques

Le nombre d'attaques sur les infrastructures critiques progresse également très fortement (+40% entre 2012 et 2013) et le type d'infrastructure visé, et donc à protéger augmente aussi. Ainsi les infrastructures dans les domaines suivants font l'objet d'une surveillance accrue :

- Information et communication
- Finance
- Aviation
- Ferroviaire
- Electricité
- Gaz
- Services gouvernementaux et administratifs
- Services médicaux
- Eau
- Services logistiques

Mais également :

- Usines chimiques
- Cartes de crédits
- Pétrole et sources d'énergie

Explosion du nombre de cibles potentielles

Le nombre d'objets connectés étant en augmentation constante et allant en se diversifiant, ce sont autant de nouvelles cibles potentielles pour les cybercriminels.

En effet la pénétration toujours plus importantes des objets connectés « classiques » de type smartphones, tablettes, ordinateurs est couplée à une augmentation des nouveaux objets comme les montres connectées, voitures de plus en plus informatisées (voire autonome)

La plupart des attaques sont étrangères

97% des attaques reçues par le Japon[24] auraient pour origine un pays extérieur. Cette pression venue de l'extérieur du pays montre la globalisation du risque informatique et complexifie les relations diplomatiques (avec la possibilité d'attaques soutenues par les gouvernements étrangers).

La géopolitique locale ne peut être négligée à cet égard. Ainsi la Chine, la Russie et la Corée du Nord ciblent le Japon afin notamment de tester ses capacités.

De manière générale, le Japon est une cible « de valeur » militaire, économique et technologique et la vulnérabilité du Japon est exacerbée par son isolation insulaire.

[24] 97% des malwares détectés en 2013 au Japon ont essayé de se connecter à des serveurs situés à l'étranger – Source : NISC

D'après Deloitte[25], le Japon a un index de vulnérabilité cyber 9 fois plus important que ses voisins asiatiques (index mesuré à partir de divers paramètres liés à la dépendance à internet). Un autre problème majeur du Japon provient du fait qu'une grande partie de la population japonais est peu informé ou se sent peu concerné par ce sujet.

Les criminels cyber japonais ont tendance à acheter des logiciels malveillants à des acteurs étrangers depuis l'Internet profond pour les utiliser au Japon pour des activités criminelles comme de l'extorsion d'argent, notamment visant les séniors, qui ne connaissent que peu le sujet[26].

Depuis 2010, le Japon a toutefois pris conscience de ses vulnérabilités, suite à une série de cyber-attaques de grande ampleur ayant touché tant les réseaux étatiques (Diète, MOFA, ambassades) que les systèmes de grands groupes industriels (dont MHI – Mistubishi Heavy Industries et Sony).
Début 2014, c'est au tour de l'Agence japonaise de l'énergie atomique (JAEA) de révéler que l'un des ordinateurs de la salle de contrôle du réacteur à neutrons rapides de Monju (alors à l'arrêt) a été infecté par un virus informatique. Enfin, en 2015 l'attaque du fond de pension japonais, durant lequel 1,25 million de dossiers de données personnelles ont été dévoilés[27]a été un élément moteus de la prise de conscience du grand public.
Ces différentes attaques ont fait réaliser au Japon l'importance de la sécurité des infrastructures dites critiques.

Enfin, le Japon voit dans les Jeux Olympiques, qu'il ambitionne comme la démonstration de son excellence technologique, un danger considérable en terme de cyber attaques[28], notamment avec l'émergence annoncée de l'IoT et des voitures autonomes à cette période.

[25] http://www2.deloitte.com/sg/en/pages/public-sector/articles/deloitte-2016-asia-pacific-defense-outlook.html

[26] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-japanese-underground.pdf

[27] http://www.reuters.com/article/us-japan-pensions-attacks-idUSKBN0OH1OP20150601

[28] http://asia.nikkei.com/magazine/20160303-INDIA-S-STARTUPS-THE-GREAT-DISRUPTORS/Tech-Science/Japan-s-cyberwarriors-gird-for-a-fight-ahead-of-the-2020-Olympics?page=2

## 2. Stratégie de cybersécurité japonaise

A l'initiative des membres du Parlement, un « Basic Act » sur la cybersécurité a été promulgué au Japon (en application depuis le 9 Janvier 2015) avec plusieurs objectifs : définir dans la loi le terme de « cybersécurité », proposer des principes de base pour la promotion de mesures pour la cybersécurité, poser un fondement légal pour établir la stratégie nationale concernant la cybersécurité et réformer le cadre institutionnel pour améliorer la cybersécurité nationale.

Ce « Basic Act » permet donc l'établissement de la stratégie japonaise par le gouvernement, afin de clarifier les objectifs gouvernementaux ou les aspects liés aux assurances, en particulier dans les infrastructures critiques.

Les principes fondamentaux sont :

- Assurer la libre circulation de l'information en maintenant des réseaux de communication avancés à travers la coopération de tous les acteurs
- Implémenter la maintenance d'Internet
- Jouer un rôle majeur dans l'effort international (notamment pour l'établissement de règles communes)
- Ne pas empiéter sur les droits des citoyens de manière abusive
- Améliorer la prise de conscience des citoyens sur les risques liés à la cybersécurité

Sur ce dernier point, plusieurs actions sont menées par le gouvernement pour sensibiliser les habitants, les entreprises et les collectivités aux menaces informatiques et pour les préparer en cas d'attaques (mois de la cybersécurité en Mars 2015, concours de hacking, etc.).

Le « Basic Act » renforce également la place de la cybersécurité avec l'affectation directe des quartiers généraux stratégiques pour la cybersécurité (***Cybersecurity Strategic Headquarters***) sous l'autorité directe du Cabinet Office (et non plus des quartiers généraux pour les technologies de l'information), dont les fonctions sont :

- Formuler la stratégie cybersécurité du Japon
- Evaluer les mesures de cybersécurité par les organismes gouvernementaux (incluant l'audit)
- Evaluer les incidents cybers sérieux dans les organismes gouvernementaux (incluant les investigations sur les causes)
- Coordonner de manière globale les politiques de cybersécurité (incluant la formulation des indications pour l'estimation du budget)

Le secrétariat de ces quartiers généraux est affecté au ***National center of Incident readiness and Strategy for Cybersecurity*** **(NISC)**, qui constitue l'autorité nationale de cybersécurité. Aujourd'hui composé d'une centaine de personnes détachées du MOD, du MIC, du MOFA, du METI et la NPA, le NISC se transforme petit à petit en « Cyber Security Center » doté de moyens accrus.

Les fonctions assurées par le NISC sont principalement :

- GSOC (*Government Security Operations Coordination team*)
- Investigation sur les causes lors d'incidents cyber importants
- Audit, consultation, expertise pour les organismes gouvernementaux
- Planification des programmes et coordination pour assurer la cybersécurité

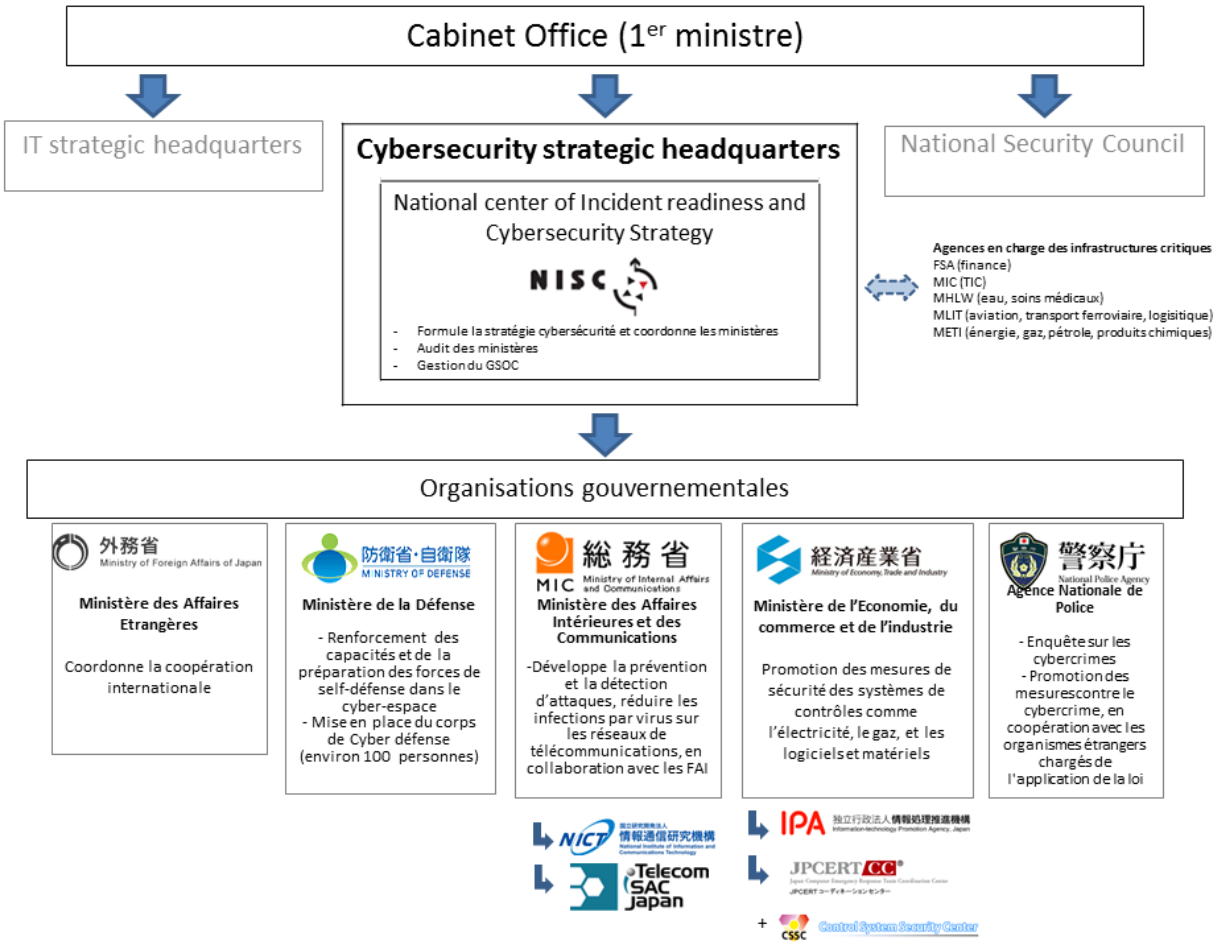



Figure 5 : Organisation et rôle du NISC

Le NISC, qui mène régulièrement des campagnes de sensibilisation auprès du secteur public, privé et universitaire, opère en interaction étroite avec trois types d'acteurs :

- Les **administrations japonaises** : le NISC formule la stratégie en cybersécurité et assure la coordination interministérielle sur cette question. De plus, au sein du NISC, l'équipe de la *Gouvernment Security Operation Coordination* (GSOC) assure la supervision continue des réseaux gouvernementaux et la diffusion des informations en cas de problème détecté. En outre, depuis 2012, la *Cyber Incident Mobile Assistant Team* (CYMAT), dont l'existence n'est pas permanente, se constitue sur une base *ad hoc* pour assister une administration affectée par un problème de cyber-sécurité dans sa recherche d'une solution.
- Le **monde de l'entreprise** : dix secteurs sont définis comme relevant des infrastructures critiques (ICT, finance, aéronautique, secteur ferroviaire, électricité, gaz, services

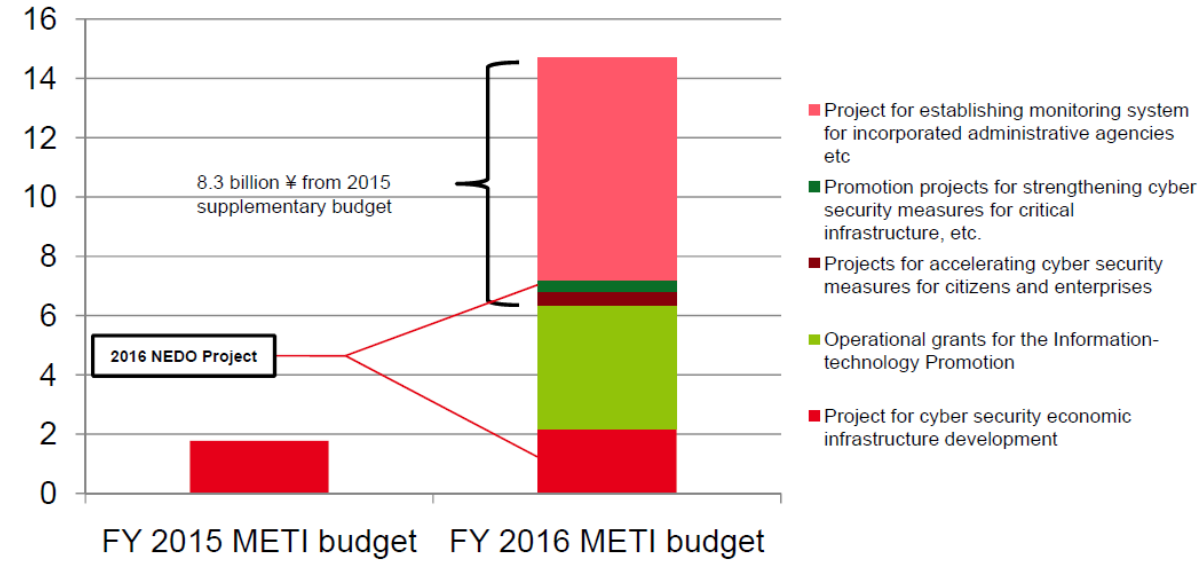
gouvernementaux, services médicaux, eau, logistique) et soumis à des obligations accrues de protection pour faire face à l'éventualité de cyber-attaques ou de catastrophes naturelles. Cette liste devrait être étendue, courant mars, aux industries pétrochimiques et au secteur des cartes de crédit. Conscient de la forte dépendance du Japon aux produits étrangers, le gouvernement s'est par ailleurs fixé pour objectif de doubler d'ici 2020 la taille de son marché domestique de la sécurité informatique.

- Les **gouvernements étrangers et les organisations internationales**, en lien étroit avec le MOFA.

Pour faire face aux cybermenaces accrues, le Japon renforce progressivement son dispositif national de surveillance et de protection des réseaux informatiques. Pour ce faire, chaque ministère s'efforce également de renforcer ses capacités internes, en fonction de ses besoins propres.
L'organisation intra gouvernementale est complexe puisque les enjeux de cybersécurité concernent tous les ministères et organisations.

- La NPA (National Police Agency) dispose depuis 2012 d'une **unité spéciale de lutte contre la cybercriminalité**.
- Le MOD a acté la création d'une **unité spécialisée dans la cyberdéfense**, d'environ 100 membres, au sein des Forces d'auto-défense (budget de 200 millions de dollars, dont la moitié consacrée au renforcement des réseaux de transmission).
- *L'Information technology Promotion Agency* – IPA, agence de promotion de l'IT mise en place par le METI et le MIC, possède un axe fort de **promotion de la sécurité informatique auprès des PME**. Les deux ministères ont également contribué en 2012 à l'établissement d'un centre spécifique de R&D et de test des infrastructures informatiques privées et de contrôle des infrastructures critiques (***Control System Security Center*** – CSSC[29]) au sein duquel collaborent 32 grandes entreprises et institutions (Hitachi, Mitsubishi, Fujitsu, NEC, Omron, Université du Tohoku, etc.) ainsi que des membres partenaires (Tokyo Gas, Préfecture de Miyagi, Fukushima Information Processing Center, etc.).

[29]http://www.css-center.or.jp/en/aboutus/




Source : METI-related budget outline FY2015 – FY2016

- Le MOFA, enfin, a créé en 2012 un poste de coordonnateur cyber avec rang d'Ambassadeur (*Ambassador in charge of Cyber Policy and UN affairs*), dont la fonction est aujourd'hui exercée par M. Koichi Mizushima, qui a pris la suite de M. Makita SHIMOKAWA (depuis juillet 2015)[30].

Le MIC à travers le bureau pour la sécurité TIC, a un rôle particulier dans cette organisation. Il a pour rôle notamment de promouvoir la détection des attaques et la prévention, ainsi que la réduction des infections par virus, sous l'angle de la protection les réseaux de télécommunications à travers la collaboration avec les FAI – Fournisseurs d'accès internet.

Pour cela, le MIC s'appuie sur deux acteurs principaux :

- Le NICT (*National Institute for Communication Technologies*)
- Telecom ISAC (*Information Sharing and Analysis Center*) Japan

Ses actions principales sont:

- Assurer la fiabilité des réseaux de télécommunications
- Etablir un environnement réseau sécurisé : partage d'information avec les FAI (Fournisseurs d'Accès Internet), renforcement les partenariats publics-privés, organisation de réunions du comité consultatif en sécurité de l'information (depuis 2013), organiser des conférences pour mettre en place des contremesures adaptées par les opérateurs
- Aide pour la mise en place de mesures de sécurité de l'information et du développement des technologies cyber : programmes ACTIVE（*Advanced Cyber Threats response InitiatiVE*;

[30] http://www.mofa.go.jp/press/release/press4e_000813.html

CYDER (*CYber Defense Exercise with Recurrence*) ; PRACTICE (*Proactive Response Against Cyber-attacks Through International Collaborative Exchange*)

- Promotion de la collaboration internationale à travers le partage des informations de sécurité (pour le moment avec les Etats-Unis et l'ASEAN, avec qui le Japon a commencé l'opération "*Japan-ASEAN Security PartnERship*").
- Garantir la bonne utilisation des données personnelles : promouvoir un bon usage/distribution des données personnelles en assurant la protection de la vie privée.

Le comité de conseil consultatif sur la cybersécurité conseille le MIC sur les contremesures dans le domaine de la sécurité TIC, notamment pour les partenariats public-privé, les grandes directions R&D qui concernent la sécurité de l'information et les actions rapides à mener en cas d'attaque (par exemple DDoS ou fuite d'information). Ce comité est présidé par le professeur Hideyuki Tokuda de l'Université de Keio.

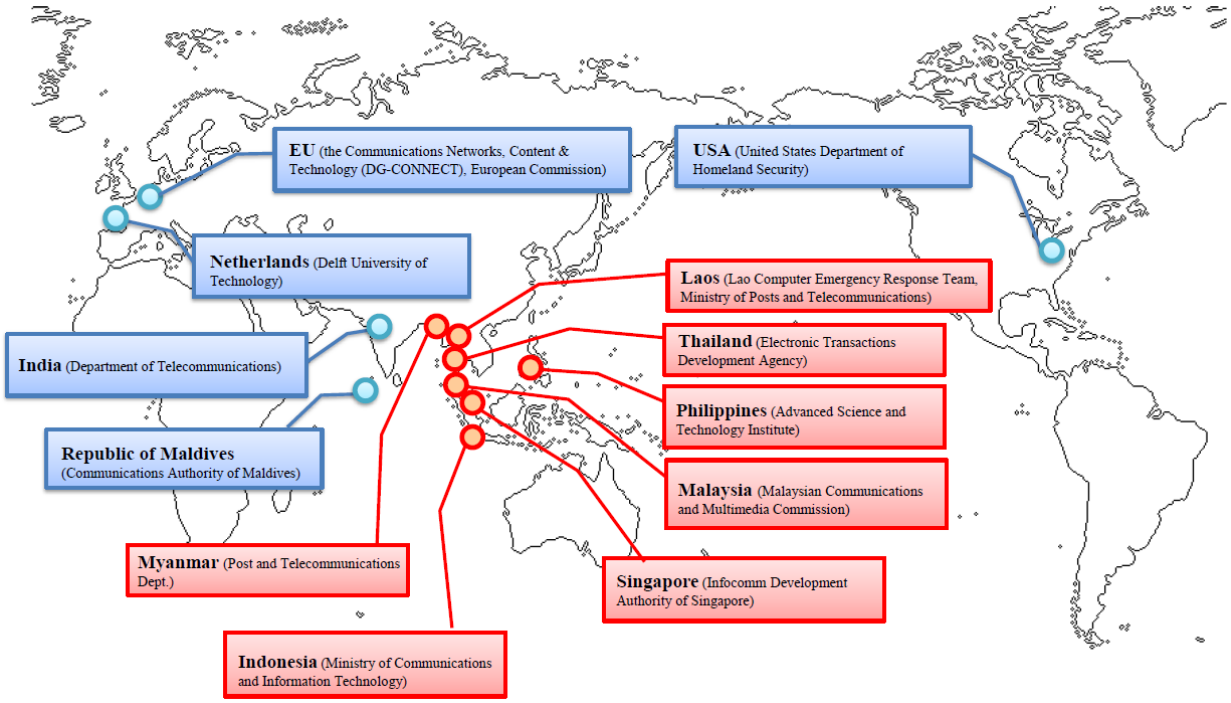



Figure 6: Principales collaborations du MIC

En juin 2013, il publie sa première **stratégie nationale de cybersécurité**, complétée en octobre 2013 par un volet spécifiquement dédié à la coopération internationale.

Le Japon, après avoir réorganisé son administration à travers le Cybersecurity Basic Act, a publié sa stratégie sur la cybersécurité fin 2015 dont les principaux objectifs sont :

| **Améliorer la vitalité socio-économique and le développement durable** | **Construire une société sûre et sécurisée pour les citoyens** | **Assurer la paix et la stabilité de la communauté internationale et la sécurité nationale** |
|---|---|---|
| « La cybersécurité n'est pas un coût, c'est un investissement »<br>- Création de systèmes IoT sécurisés<br>- Promotion de la gestion d'entreprise prenant en compte la sécurité<br>- Amélioration des conditions des affaires en cybersécurité | « Développement d'infrastructures cyber pour 2020 et au-delà »<br>- Mesures pour la protection des personnes et de la société<br>- Mesures pour la protection des infrastructures critiques<br>- Mesures pour la protection des organisations gouvernementales | « Contribution proactive à la paix dans le cyber-espace »<br>- Assurer la sécurité nationale<br>- Maintenir la paix et la stabilité à l'échelle internationale<br>- Coopération et collaboration avec les autres pays |
| **Approches transverses pour la cybersécurité** | | |
| Progrès de la R&D | Développement des capacités des employés | |

Le NISC a enfin entamé la réalisation d'un cadre général pour des systèmes IoT sécurisés ("*General Framework for Secured IoT Systems*"[31]). En effet le NISC souhaiterait que les industriels de l'IoT intègrent l'idée de « Sécurité par le design » (« Security by design »).

Le NISC a entamé une consultation publique de son modèle pour vérification et amélioration[32].

L'organisme de lutte contre les incidents cyber : JP CERT (*Japan Computer Emergency Response Team*)

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

[31] http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf

[32] http://www.nisc.go.jp/eng/iot_framework2016.html

Le JPCERT[33] est le premier CSIRT (*Computer Security Incident Response Team*) à avoir été mis en place au Japon. L'organisation travaille en coordination avec les FAI, les fournisseurs de solutions de sécurité, les agences gouvernementales, ainsi que les associations industrielles. Il agit ainsi comme coordinateur des différents CSIRTs japonais.

Ses activités sont ainsi :

- Réponse en cas d'incident et analyse
- Alertes de sécurité
- Coordination des autres CSIRTs
- Coordination des fournisseurs de sécurité
- Education et formation
- Recherche et analyse

Dans la région Asie-Pacifique, le JPCERT a contribué à l'établissement de l'APCERT[34] (*Asia Pacific Computer Emergency Response Team*), dont il assure les fonctions de secrétariat.

Le JPCERT gère également le conseil anti-hameçonnage japonais (*Council of Anti-Phishing Japan* (APC)).

Le Conseil japonais contre le *fishing* a lancé une plateforme pour renforcer la prise de conscience japonaise sur les affaires cyber et les comportements à risque sur Internet, appelée stopthinkconnect.jp[35]. Les membres de ce groupe sont :

- BB Softservice Corp.
- RSA, The Security Division of EMC
- GMO GlobalSign K.K.
- Alps System Integration Co., Ltd.
- Kaspersky Labs Japan
- Hitachi Systems, Ltd.
- SOURCENEXT CORPORATION
- Trend Micro Incorporated
- TOPPAN FORMS CO., LTD.
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

C'est la première campagne de ce genre réalisée dans une langue autre que l'anglais (ce projet est historiquement développé par la *National Cyber Security Alliance* – NCSA américaine).

[33] http://www.jpcert.or.jp/english/

[34] http://www.apcert.org/

[35] http://www.businesswire.com/news/home/20141210006258/en/Council-Anti-Phishing-Japan-Launches-STOP.-THINK.-CONNECT.

## 3. Les principaux acteurs de la cybersécurité au Japon

L'industrie japonaise a globalement pris du retard sur ses homologues internationaux sur les questions de cybersécurité.

Depuis les cyberattaques spectaculaires qui ont marqué l'actualité de ces dernières années, le gouvernement japonais a pris conscience des insuffisances nationales en matière de cybersécurité. C'est pourquoi désormais de grandes initiatives ont vu le jour afin de consolider les compétences et la sécurité des infrastructures.

### a. Le marché de la cybersécurité au Japon

Le marché de la cybersécurité japonais suit la tendance de croissance mondiale. En 2015, le marché japonais était d'environ 8,5 milliards d'euros

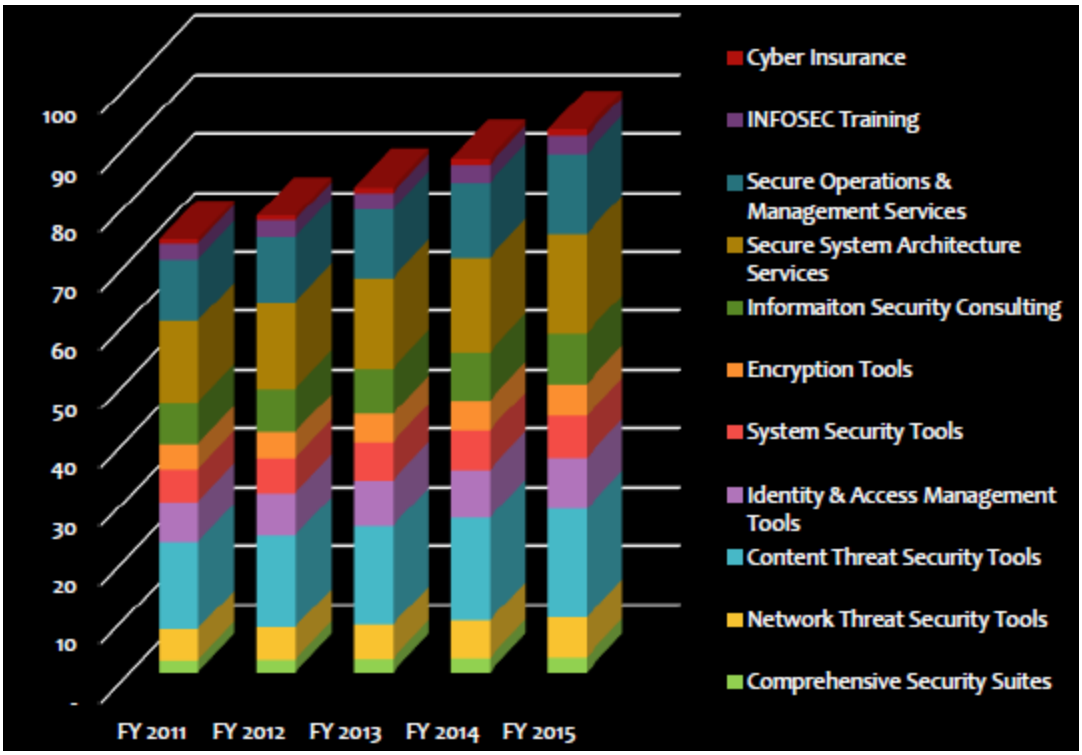



Figure 7 : estimations et historique du marché de la cybersécurité au Japon[36]

[36] Etude Infosec

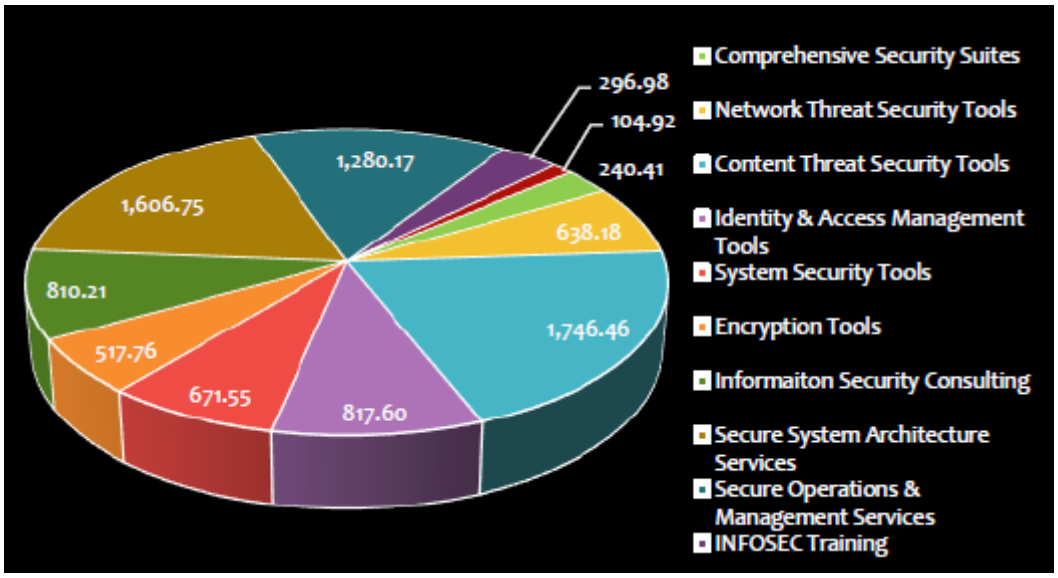



Figure 8 : distribution par type de produits

**La formation est un des problèmes majeur du Japon**. Les industriels et le gouvernement font face à un manque de main d'œuvre qualifiée dans le domaine. D'après William Saito, conseiller spécial pour la politique scientifique et technologique auprès du gouvernement japonais (de nationalité américaine), il manque au moins 80000 professionnels de la cybersécurité au Japon.
Pour pallier à ce problème le gouvernement japonais fait appel à ses ressources internes, s'appuie sur ses partenaires privés majeurs (NEC, Fujitsu, etc.) et compte également sur l'aide internationale pour développer ses capacités.

Afin de renforcer ses capacités, le NISC a notamment décidé d'engager une dizaine de « white hat hackers » (des hackers qui ont décidé d'agir pour l'intérêt commun). Le gouvernement cherche à recruter des professionnels du secteur privé[37].

Le Keidanren[38] a également rassemblé un groupement d'une trentaine de sociétés pour travailler sur les questions de cybersécurité. Il a également inscrit dans sa politique un paragraphe sur l'importance de la cybersécurité et de la collaboration publique-privée, la nécessité de s'accorder à développer des solutions technologiques, d'améliorer la formation et la prise de conscience des dirigeants d'entreprise sur ces problématiques[39].

[37] http://www.japantimes.co.jp/news/2015/03/09/national/nisc-to-begin-hiring-white-hat-hackers-in-fiscal-2015/#.Vgn8Jlo6fK0

[38] Fédération des organisations économiques japonaises

[39] http://www.keidanren.or.jp/policy/2015/054.html

Pour renforcer la prise de conscience japonaise de l'importance de la cybersécurité et des lacunes actuelles du pays, de plus en plus d'évènements nationaux et internationaux ont lieu au Japon autour de la cybersécurité. Dans les salons non-dédiés mais avec un sujet proche, on retrouve souvent une thématique sur le sujet cyber dans les conférences, notamment :

- International Workshop on Security (IWSEC) : http://www.iwsec.org/
- CEATECH Japan (volet sur la cybersécurité) : http://www.ceatec.com/ja/

### b. Principaux industriels japonais de la cybersécurité

Plusieurs entreprises japonaises mettent en place des solutions dans le domaine de la cybersécurité. Toutefois, l'offre reste essentiellement basée sur les couches hautes des technologies, et reste peu développée sur les aspects hardware.

| **Nom de la société** | **Technologies et projets majeurs** |
|---|---|
| NTT Group | Plusieurs organisations travaillent sur le cyber :<br>- NTT Docomo<br>- NTT Data<br>- NTT communications<br>- NTT secure platform Lab<br><br>Techniques de visualisation des attaques<br><br>NTT-CERT: *NTT Computer Security Incident Response and Readiness Coordination Team* |
| NEC | Solutions de cybersécurité de NEC :<br>http://jpn.nec.com/cybersecurity/pdf/NEC_CyberSecuritySolutions_en.pdf<br><br>Filiales :<br>- Cyberdefense Institute<br><br>Evaluation de vulénrabilité, tests de pénétration, réponse aux incidents<br>- Infosec<br><br>Security management et consulting<br><br>Partenariats :<br>- Gold partner pour les Jeux Olympiques<br>- Exercices en coopération avec le gouvernement japonais (MIC)<br>- Coopération avec Interpol (Singapour) |

| | |
|---|---|
| | - partenariat pour la formation avec JAIST (Kanagawa)<br>- LAC Co., Ltd.<br>- FFRI, Inc.<br>- Trend Micro Inc.<br>- NRI Secure Technologies, Ltd.<br>- S&J Corp. |
| Fujitsu | Détection des intrusions & prévention des infections:<br>http://www.fujitsu.com/uk/Images/reducing-the-risk-of-business.pdf<br><br>Plateforme de sécurité automatisée et autonome (Intelligence artificielle, Machine learning)<br>- Systèmes réseaux (5G, réseaux de capteurs/ réseaux photoniques)<br>- Conceptions logicielle et matérielle<br>- Analyse comportementale et psychologique des utilisateurs pour identifier des vulnérabilités<br><br>Partenariats :<br><br>- Université de Tokyo<br>- Université d'Electro-Communications de Tokyo<br>- Partenaires industriels : #becrypt, Cisco, FireEye, Mc Afee, Juniper, Trend Micro, BAE systems, etc. |
| Hitachi | Solutions cyber de Hitachi :<br>http://www.hitachi.com/rev/pdf/2016/r2016_08_108.pdf<br><br>Partenariats :<br><br>- Université de Keio (IoT et cybersécurité)<br>- HP (partage d'intelligence) |
| Toshiba | Partenariats :<br><br>- Intel[40] (partenariat por l'IoT)<br>- British Telecom (quantum cryptographie[41]) |
| FFRI Inc. | Solutions de FFRI : http://www.ffri.jp/products/index.htm<br><br>- Systèmes d'analyse automatiques de logiciels malveillants<br>- Sécurité du navigateur |

[40] https://www.toshiba.co.jp/about/press/2015_09/pr1601.htm

[41] http://www.computing.co.uk/ctg/news/2428904/toshiba-and-bt-boast-unhackable-network-security-with-new-quantum-cryptography-tech

| | |
|---|---|
| Trend Micro | TM cybersecurity solutions : http://cloudsecurity.trendmicro.com/us/technology-innovation/cyber-security/ |
| Nomura Research Institute (NRI) | Partenariat avec *Tokyo Institute of Technology*[42] pour la formation et les technologies de défense contre les cyberattaques |
| KDDI | *KDDI Research Institute* et *KDDI labs*<br><br>Quelques solutions de sécurité KDDI : http://www.kddi.com/english/business/cloud-network-voice/security/<br><br>Partenariats:<br>- FireEye |
| Trillium | Sécurité de l'IoT (basé sur des solutions logicielles) : http://www.trillium.co.jp/#section-about-brooklyn |
| … | … |

**Telecom ISAC (Information Sharing and Analysis Center)**

Telecom ISAC travaille en étroite collaboration avec le MIC et les FAI pour assurer la sécurité des réseaux de télécommunication au Japon.

Ses missions principales sont :

- Mettre en place des groupes de travail pour les problèmes communs aux FAI et aux acteurs de l'industrie des télécommunications
- Organiser des évènements, des exercices cyber et les réunions d'avancement pour les partenaires
- Opération du système de surveillance des routes « Keiryo-Bugyo » (groupe de travail BGP)
- Opération du système d'observation des infrastructures critiques
- Coopération et collaboration avec les organismes externes (MIC, NISC, NICT, JPCERT/CC, etc.)
- Gestion du programme « ACTIVE »
- Participation au programme « PRACTICE »
- Education et développement des technologies pour la sécurité

[42] https://www.nri.com/global/news/2016/160510_1.aspx

Les sociétés membres du consortium sont:

- NEC Corporation
- NTT Communications Corporation
- KDDI Corporation
- Internet Initiative Japan Inc.
- Nifty Corporation
- Hitachi, Ltd.
- Oki Electric Industry Co., Ltd.
- Softbank Corp.
- Nippon Telegraph and Telephone East Corporation
- Nippon Telegraph and Telephone West Corporation
- Nippon Telegraph and Telephone Corporation
- KDDI R&D Laboratories
- BIGLOBE Inc.
- Fujitsu Limited
- Internet Multifeed Co.
- NTT DOCOMO, INC.
- NTT DATA INTELLILINK CORPORATION
- So-net Corporation
- NTT Com Security (Japan) KK
- K-Opticom Corporation

Telecom ISAC est composé de 12 groupes de travail, travaillant sur les sujets prioritaires identifiés[43].

**IPA (Information-technology Promotion Agency)**

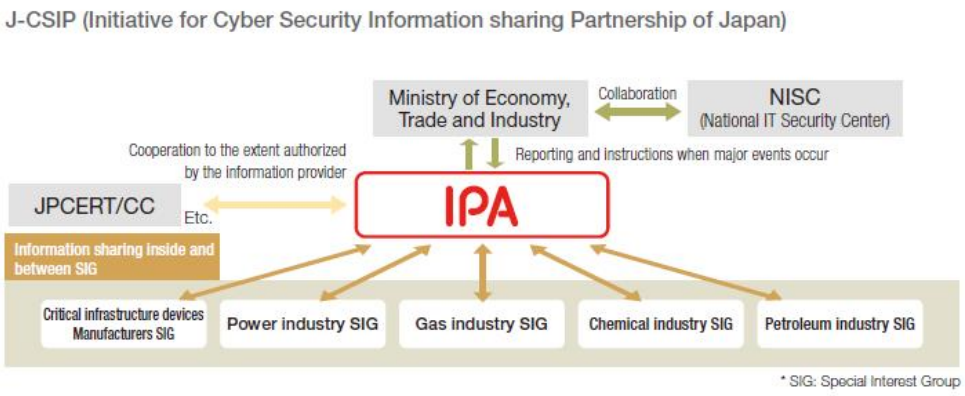



Figure 9 : organisation d'IPA

[43] https://www.telecom-isac.jp/english/#organization


Figure 10 : les trois missions principales d'IPA

IPA a tout d'abord une mission d'information auprès du grand public. IPA est ainsi auteur de grandes campagnes de communication grand public autour des problèmes de la sécurité informatique individuelles. IPA réalise ces opérations au Japon, mais également en ASEAN[44].


Figure 11 : Exemple de champagne de communication de l'IPA

IPA mène également des activités de recherché sur la cryptographie (CRYPTREC[45]), l'évaluation des certifications et la standardisation :

- Cryptography for Secure Network Society
- Maintenance of the e-government recommended ciphers list:
- Evaluation of cryptographic modules
- Contribution to international standardization

[44] http://www.nisc.go.jp/aj-sec/index.html

[45] http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html

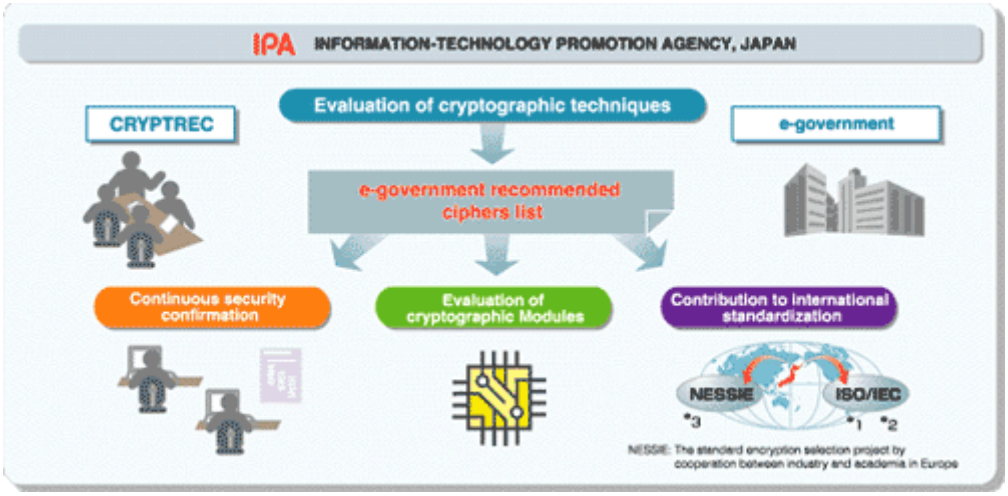



Figure 12 : Evaluation des procédés cryptographiques par IPA

Enfin, IPA travaille à renforcer la sécurité des logiciels à travers des mécanismes de prévention et de certification, en lien avec les parties prenantes japonaises et internationales[46].

Pour les standards de sécurité IT, IPA et le Japon utilisent la norme ISO/IEC 15408 (Common Criteria).

[46] http://www.ipa.go.jp/english/about/outline/security/01.html

### c. Les principaux acteurs de la recherche japonaise

Du point de vue des publications[47], les principales institutions japonaises sont listées dans le tableau suivant :

| | Institution | Scholarly Output |
|---|---|---|
| 1 | University of Tokyo | 242 |
| 2 | Nippon Telegraph & Telephone | 223 |
| 3 | Kyushu University | 189 |
| 4 | Japan National Institute of Information and Communications Technology | 179 |
| 5 | National Institute of Advanced Industrial Science and Technology | 162 |
| 6 | Waseda University | 143 |
| 7 | University of Electro-Communications | 123 |
| 8 | Tokyo Institute of Technology | 109 |
| 9 | Osaka University | 104 |
| 10 | Tohoku University | 103 |
| 11 | Fujitsu | 101 |
| 12 | Keio University | 96 |
| 13 | Hitachi | 96 |
| 14 | Research Organization of Information and Systems National Institute of Informatics | 92 |
| 15 | University of Tsukuba | 81 |
| 16 | Kyoto University | 79 |
| 17 | NEC Corporation | 74 |
| 18 | Japan Advanced Institute of Science and Technology | 71 |
| 19 | Nagoya University | 64 |
| 20 | KDDI R&D Laboratories | 60 |

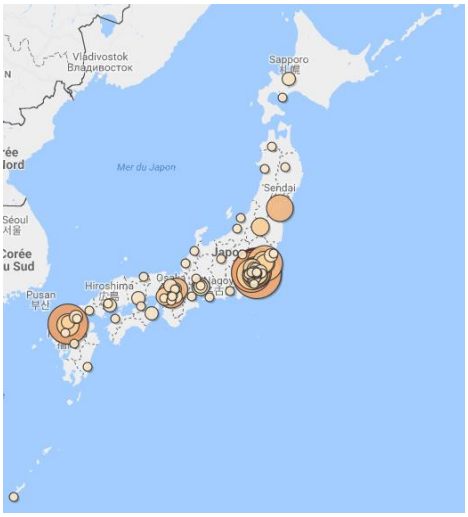



Figure 13 : carte des acteurs de la recherche japonaise en cybersécurité

[47] Données Scival (Elsevier), sur la période 2011-2015. Recherche effectuée avec le mot clé « cybersécurité » pour les revues d'informatique et d'ingénierie.

**Les thèmes de recherche au Japon**


Figure 14 : Nuage des mots-clés principaux de la recherche sur la cybersécurité au Japon[48]

**Organismes de recherche japonais**

**NICT**

Au sein du NICT, un institut dédié à la cybersécurité existe : le Cybersecurity Research Institute, organisé en trois parties :

[48] Source : étude Scival©, Elsevier, données 2011-2015


Figure 15 : Organisation de l'institut de la cybersécurité du NICT

Le *Security Fundamentals Laboratory* contribue au projet CRYPTEC (*Cryptography Research and Evaluation Committees*)[49], qui évalue les codes secrets fournis par le gouvernement et évalue la sécurité des modules cryptographiques.

**AIST (National Institute of Advanced Industrial Science and Technology)**

L'AIST est un centre de recherche pluridisciplinaire basé à Tsukuba, qui dépend du METI.

Au sein de l'AIST, l'Information Technology Research Institute (ITRI, environ 300 chercheurs, environ 7 milliards de yens de budget) aborde notamment les questions de cybersécurité.

Thèmes de recherche de l'AIST :

- Services sécurisés
  - Méthodes d'authentification sécurisée sur Internet
  - Contremesures contre les erreurs humaines
  - Codes correcteur d'erreur – mathématiques pour la fiabilité de l'information
- Systèmes de contrôles et sécurité matérielle
  - Sécurisation des systèmes de contrôles
    - Appareil de « barrière de sécurité » (SBD - Security Barrier Device)
    - Contrôle d'accès (white lists)
    - Hyperviseur
  - Evaluation de sécurité matérielle

[49] http://www.cryptrec.go.jp/english/index.html

        - SASEBO/ZUIHO/MiMICC – cartes d'évaluation pour les attaques par canaux auxiliaires
        - Fonctions physiquement inclônables (PUF - Physically Unclonable Functions) pour vérification d'unicité
- Technologies de sécurité innovantes de nouvelle génération
    - Preuves de sécurité plus sûres pour les technologies de cryptographie
    - Design et analyse de primitives cryptographiques
    - Recherche dans les bases de données en préservant la confidentialité des données
- Développement de logiciel sécurisé
    - Design de logiciel sécurisé
    - Calot (FOT) : assistant pour les tests de design utilisant l'analyse de fonctionnalités
    - SENS : développement de langages pour les systèmes de test
    - CONPASU : outils d'analyse et d'assistance pour le développement simulané de programmes
    - ModBat : un testeur basé sur des modèles (en particulier test d'API logiciels)
    - Implémentation de logiciels sécurisés
        - Génération automatique et tests pour l'implémentation de protocoles de communication
    - Assurer/Vérifier la sécurité logicielle
        - Vérifications formelles pour la sécurité logicielle. Vérifications formelles sur des programmes bas-niveau et des codes de correction d'erreur (basé sur Coq)
    - Assurer l'exécution sécurisée des logiciels
        - Sécurité logicielle en utilisant les techniques de langages de programmation (fail-safe C ; memorisafe implementation of C, etc.)
        - Techniques de virtualisation pour la fiabilité logicielle

L'AIST a par ailleurs entamé un partenariat avec le *European Network for Cyber Security* (ENCS) pour la sécurité de l'IoT, en particulier pour les infrastructures critiques.

**<u>Principaux laboratoires universitaires menant des recherches sur la cybersécurité :</u>**

Keio University

- *Cyber Security Research Center*(SU)[50] au sein du *Keio Advanced Research Center* (KARC) : Recherche conjointe avec Hitachi pour la réalisation d'une « super smart society », basée sur l'IoT et la cybersécurité[51]

Université de Tokyo

[50] http://www.karc.keio.ac.jp/center/center-54.html

[51] http://www.hitachi.com/New/cnews/month/2016/02/160229.pdf

- Matsuura Lab[52] : Cryptograpie, sécurité réseau, gestion de la sécurité
- Rie Yamaguchi Lab [53] : authentification, protection de la vie privée

Université de Kyushu

- *Institute of Mathematics for Industry* (en particulier travaux sur la cryptographie)

Fukuoka Institute of Technology

- *Information Networking and Applications Laboratory* (INA): Sécurité des données

Le JAIST (*Japan Advanced Institute of Science and Technology*) à Kanazawa est également un acteur très actif dans le domaine de l'analyse malware.

Les universités de Meiji, Tsukuba et du Tohoku sont également actives dans le domaine.

### d. Projets gouvernementaux en cours

**Protection des infrastructures critiques**

Le Japon met un accent particulier pour la protection de ses infrastructures critiques. Le Japon a ainsi mis en place un programme de recherche public-privé particulier sur le sujet (projet SIP), un centre de R&D conjoint pour ses systèmes de contrôle critiques avec des industriels (CSSC, Control System Security Center) et enfin a émis un guide de bonne pratique à destination des opérateurs d'infrastructures critiques afin qu'elles soient correctement protégées.

Projet SIP – Cybersécurité pour les infrastructures critiques

M. Atsuhiro GOTO, Professeur à l'Institute of Information Security (IISEC), a été nommé directeur du nouveau programme « Cybersécurité pour les infrastructures critiques » qui a été ajouté au programme-cadre SIP en mai 2015[54]. C'est le 11ème programme-cadre SIP[55] , géré par le Conseil pour les Sciences, la technologie et l'innovation (CSTI), qui dépend directement du Cabinet Office.

Le programme « Cybersécurité pour les infrastructures critiques » est ainsi doté de 2,5 milliards de yens pour l'année 2016 (environ 22 millions d'euros).

[52] http://kmlab.iis.u-tokyo.ac.jp/index.html

[53] http://www.yamagula.ic.i.u-tokyo.ac.jp/index_e.html

[54] site du Cabinet Office http://www.cao.go.jp/minister/1412_s_yamaguchi/photo/2015-047.html, Nikkan Kogyo le 7 août http://www.nikkan.co.jp/news/nkx0720150807eaac.html

[55] http://www8.cao.go.jp/cstp/panhu/sip_english/sip_en.html

http://www8.cao.go.jp/cstp/english/sip/elevenissues.pdf

Ce programme vise à ce que le Japon bénéficie d'infrastructures critiques compétitives soutenues par des technologies cyber avancées, notamment en vue de l'organisation des jeux olympiques et paralympiques de 2020 Il s'agit également d'améliorer l'indépendance technologique du Japon vis-à-vis des technologies cyber fondamentales dans ce domaine.

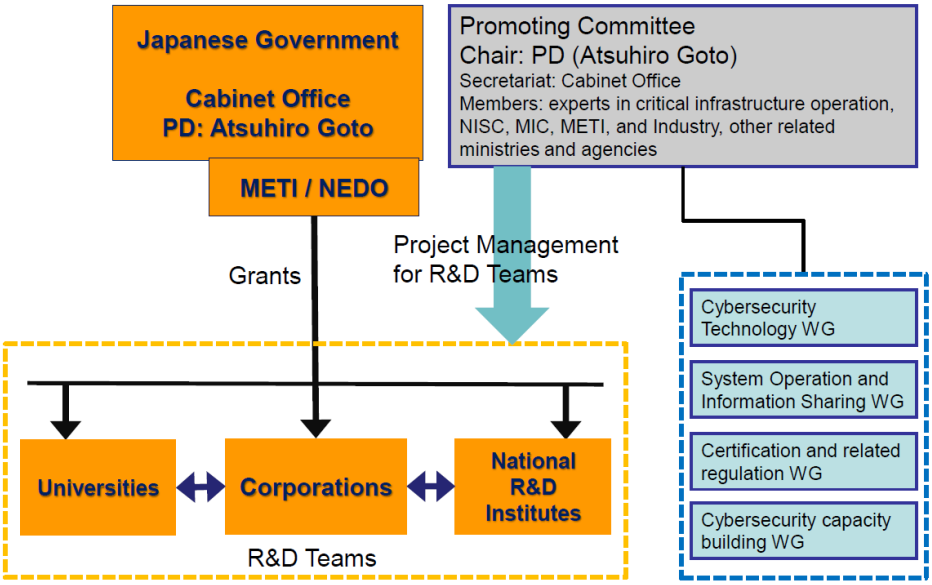



Figure 16 : Organisation du programme "cybersecurity for critical infrastructure"

Control System Security Center (CSSC)[56]

Le CSSC est situé à dans la préfecture de Miyagi et a été créé en 2012. Il est opéré sous l'autorité du METI. Il regroupe 32 entreprises et académiques[57] pour travailler en coopération sur la recherche et les tests sur les systèmes de contrôle critiques.

Figure 17 : les locaux du CSSC

Les activités principales du CSSC sont organisées autour de 4 thèmes principaux :

[56] http://www.css-center.or.jp/en/index.html

[57] http://www.css-center.or.jp/en/aboutus/index.html

- Les technologies hautement sécurisées
- Les technologies d'analyse
- Le test et la certification
- La formation

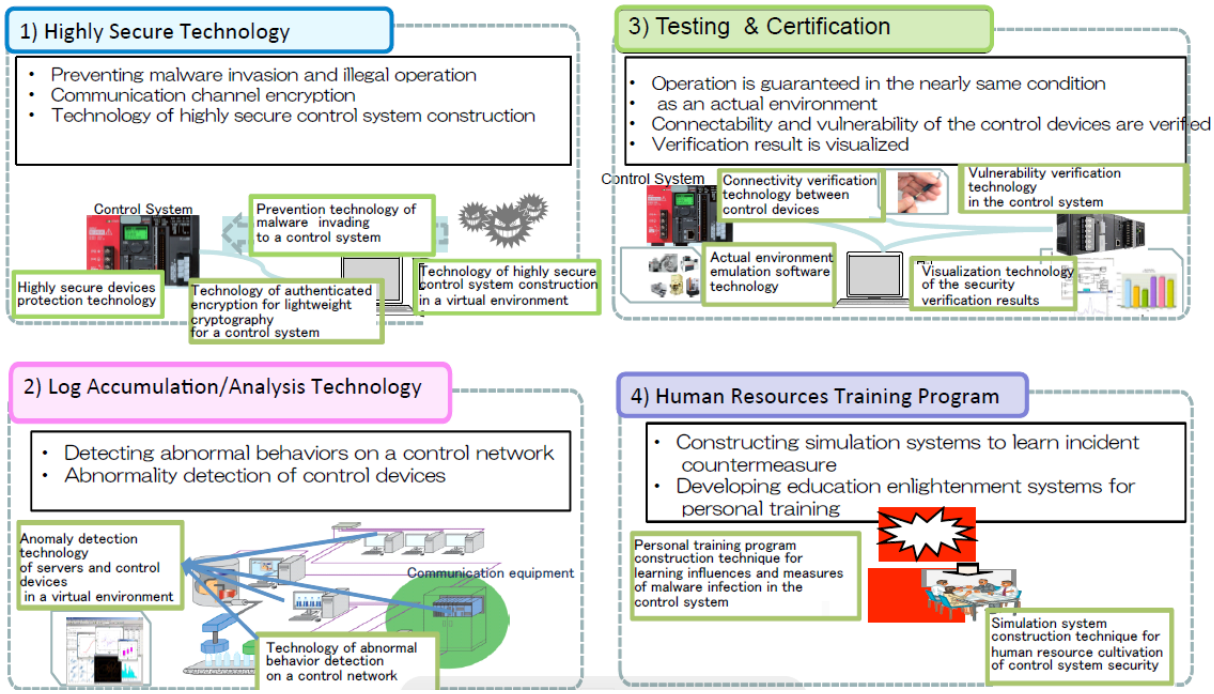



Figure 18 : panorama de la recherche au CSSC

Critical Information Infrastructure Protection guidelines

La protection des infrastructures critiques est un sujet particulièrement important pour le Japon, qui a établi en mai 2015 un plan sur « **Basic Policy of Critical Information Infrastructure Protection** [58]», qui fait suite aux deux premiers plans d'action concernant la protection de l'information des infrastructures critiques pour définir une politique commune entre gouvernement et opérateurs de ces infrastructures pour protéger en cas de désastre ou d'attaques les infrastructures critiques de coupure, de prise de contrôle malveillante ou de vol d'informations sensibles. Des procédures sont notamment mises en place en cas de crise.

[58] http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf?bcsi_scan_96404f7f6439614d=0&bcsi_scan_filename=actionplan_ci_eng_v3_r1.pdf

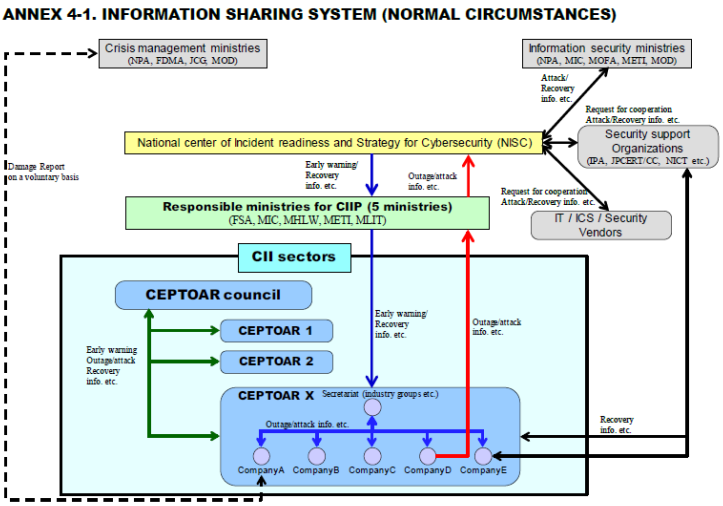



Figure 19 : mode opératoire pour les opérateurs d'infrastructure critique en fonctionnement nominal

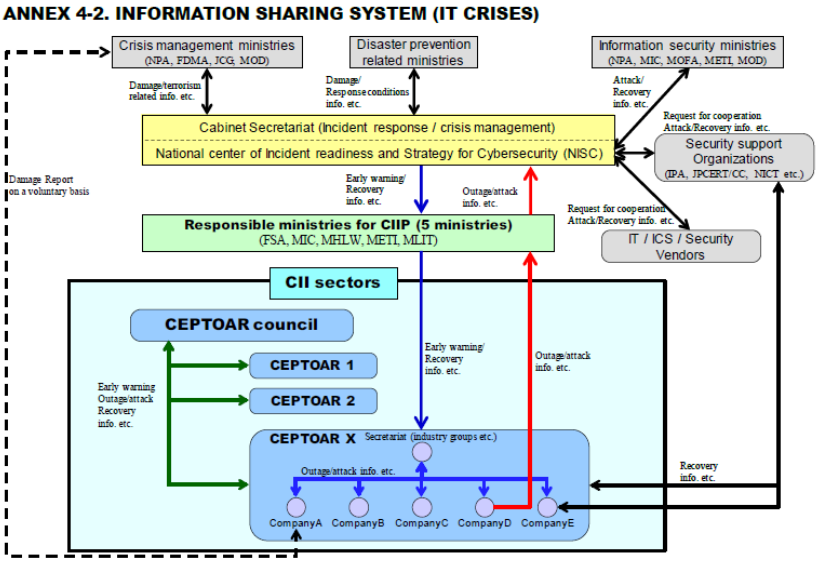



Figure 20 : mode opératoire pour les opérateurs d'infrastructure critique en cas de crise

## Projets du MIC en cours (2013-2017)

Le MIC encourage les partenariats internationaux et est à l'initiative de plusieurs projets majeurs sur la cybersécurité :

- projet ACTIVE (*Advanced Cyber Threats response InitiatiVE*) : lutte contre les infections par logiciel malveillant sur les ordinateurs individuels

- projet CYDER (*Cyber Defense Exercise with Recurrence*) : lutte contre les menaces persistantes avancées[59]
- projet PRACTICE (*Proactive Response Against Cyber attacks Through International Collaborative Exchange*) : lutte contre les attaques « malicieuses » de type déni de service (DDos) provoquées par des logiciels malveillants

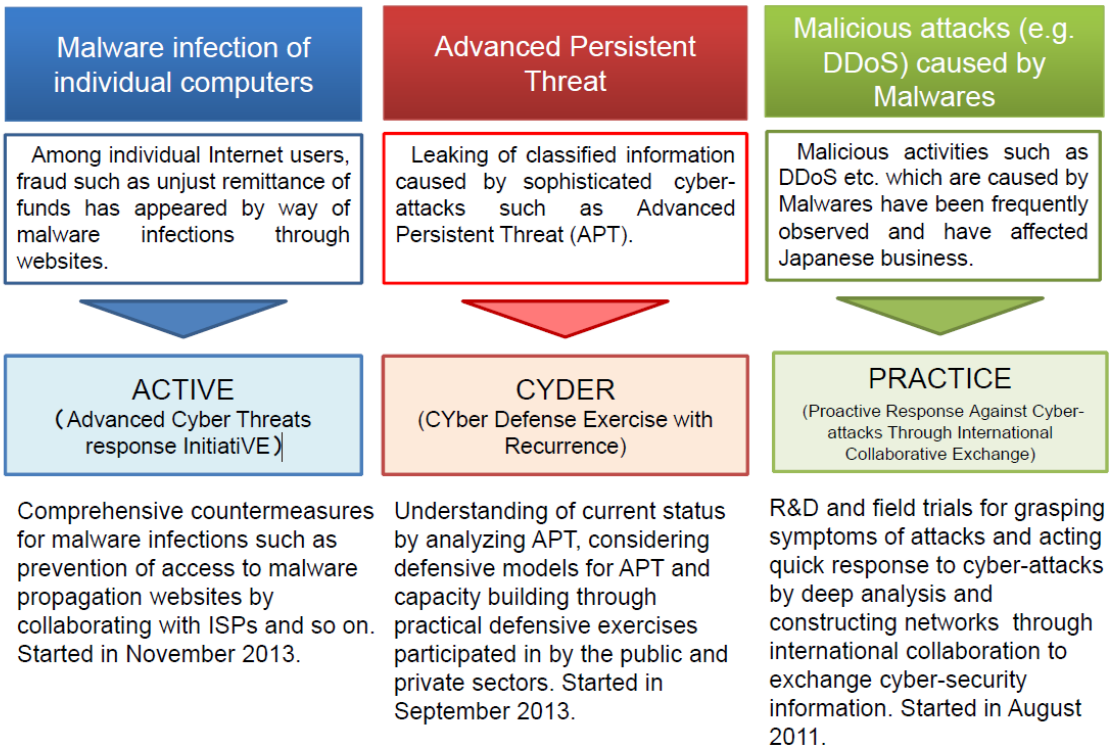


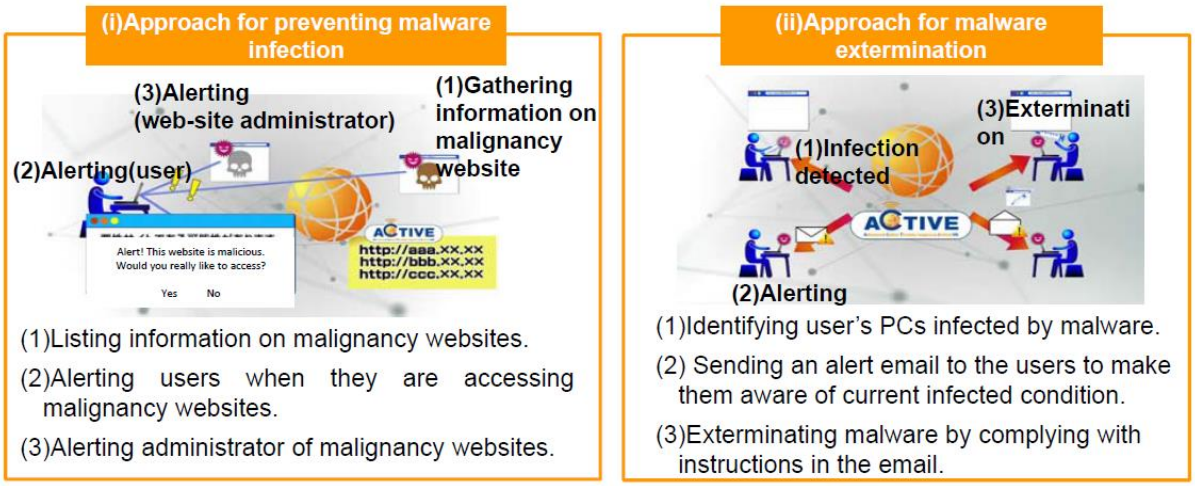

Figure 21: synthèse des principaux projets du MIC

Projet ACTIVE :

Le projet ACTIVE[60] est financé par le MIC et opéré par Telecom-ISAC, en charge de la coordination et de la planification. Il regroupe 13 FAE (Fournisseurs d'Accès Internet) et 14 sociétés.

[59] Attaque basée sur une stratégie dont l'objectif est de rester le plus longtemps possible sans éveiller les soupçons (furtivité), mettant en oeuvre de nombreuses techniques d'attaques (injection SQL, XSS, etc.)

[60] http://www.active.go.jp/en/active/

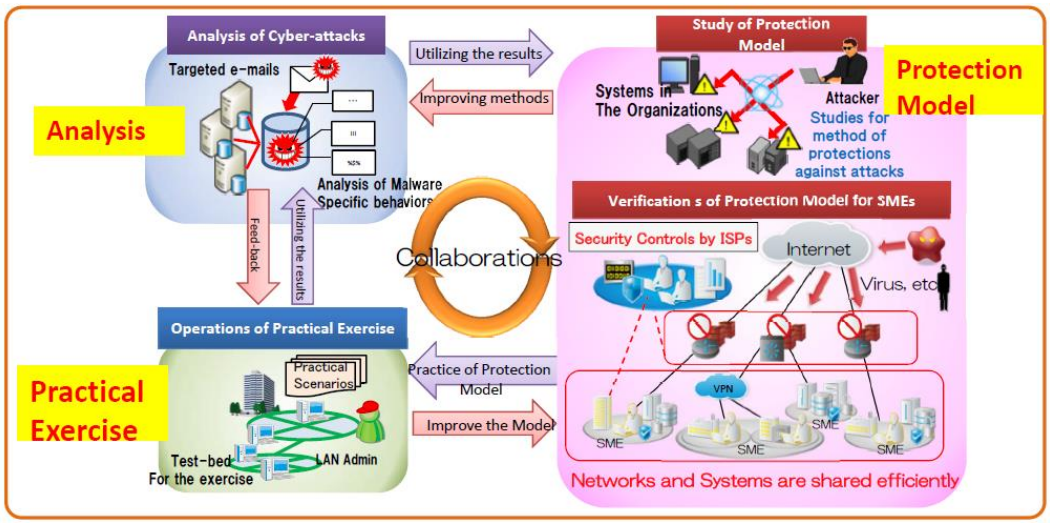


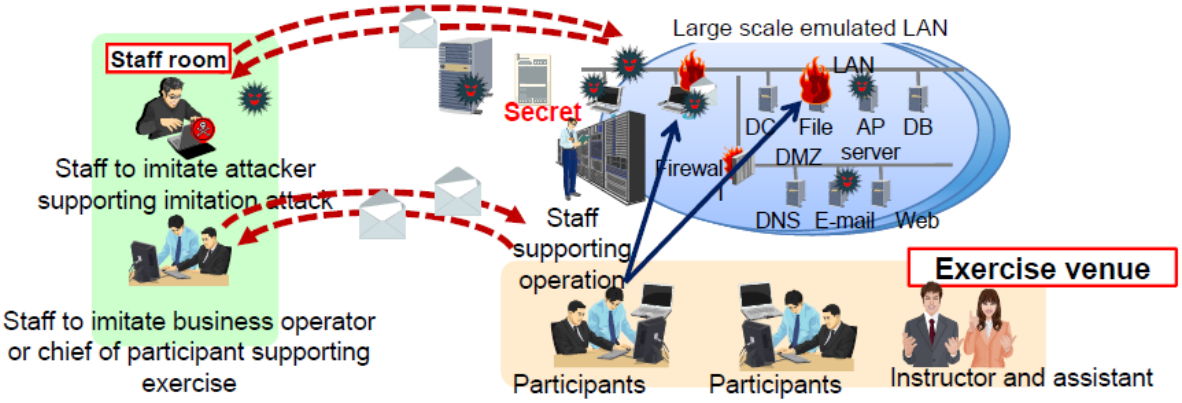

ACTIVE vise, à travers une collaboration publique-privée développée, à envoyer des alertes aux utilisateurs Internet pour prévenir les infections par les logiciels malveillants, supprimer ces logiciels et encourager les utilisateurs à prendre des mesures de manière autonome contre l'infection.

Projet CYDER (*CYber Defense Exercise with Recurrence*) :

Le projet CYDER a pour objectif d'analyser les attaques persistantes, de créer des modèles de protection et de réaliser des simulations pratiques, afin de :

- renforcer les capacités des opérateurs de LAN dans les agences gouvernementales, les grandes entreprises (environ 200 personnes de plus de 60 organisations)
- développer des modèles de défense à travers l'expérience des mises en pratiques répétées






**Program**

| | Day 1 | Day 2 |
|---|---|---|
| Morning | • Level checking of participants before exercise<br>• Introduce examples of recent cyber-attacks<br>• Explain exercise environment and tools | • Evaluation by exercise staff |
| Afternoon | • Practical training<br>Analyzing malware, confirming damage situation, making reports etc. | • Report by each group.<br>• Q&A and feedback from instructor.<br>• Examination after exercise |

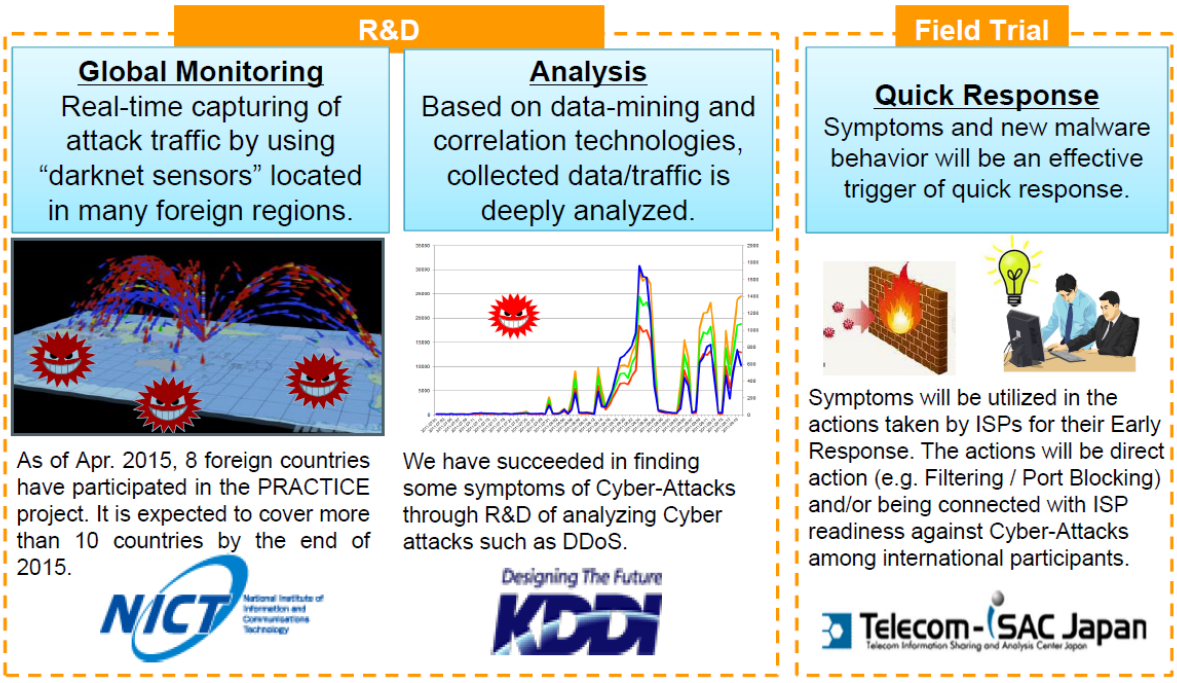
**Evaluation**

- Almost 90% of the participants say the practical training in CYDER meets their expectations
- More than 90% of the participants think the practical training in CYDER is very useful

Figure 22 : programme des exercices

Projet PRACTICE

Le projet PRACTICE vise à développer des solutions pour évaluer les symptômes et des réponses rapides aux cyberattaques, basées sur une collaboration internationale. Le Japon utilise notamment ce projet pour développer ses collaborations avec les pays d'Asie du Sud-Est.




Les partenaires principaux du projet sont le NICT, Telecom ISAC et KDDI. Les partenaires académiques du projet sont:

- *Yokohama National University*
- *Institute of Systems, Information Technologies and Nanotechnologies*
- *SecureBrain Corporation*
- *KDDI R&D Laboratories*
- *Japan Datacom Co., Ltd*

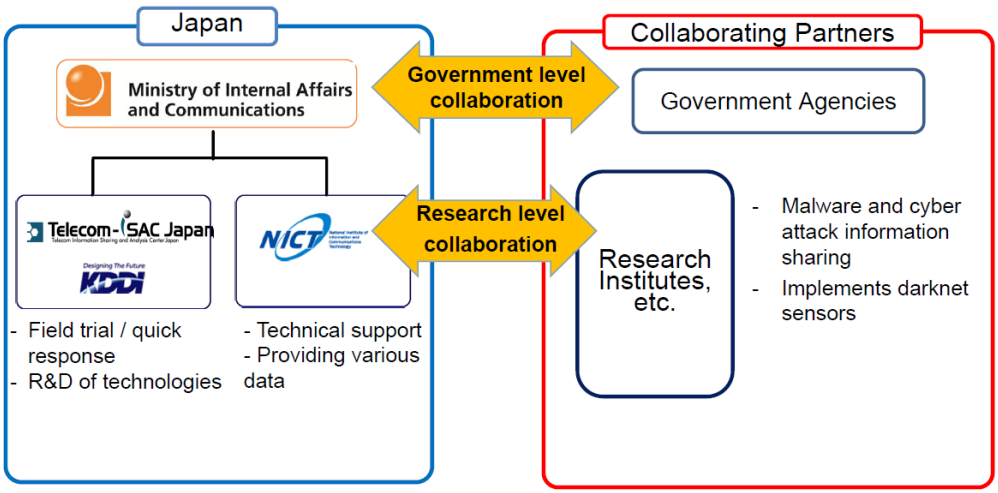



Figure 23 : Schéma de collaboration international pour le projet PRACTICE

# III. Partenariats internationaux du Japon sur la question cyber

Le Japon a accueilli en 2016 le G7. Outre le sommet des chefs d'Etats, un grand nombre de G7 ont été organisés afin de développer la coopération internationale sur des thèmes sociétaux majeurs (santé, affaires étrangères, finance, transport, science & technologie, etc.). Un G7 a notamment été dédié aux Technologies de l'Information et de la Communication (TIC), qui s'est tenu les 29 et 30 avril 2016 à Takamatsu (préfecture de Kagawa)[61].

La cybersécurité (en particulier la promotion de la cybersécurité ), a été évoquée non seulement dans le cadre du G7 TIC, mais également lors du G7 réunissant les ministres des affaires étrangères, et lors du sommet présidentiel, preuve de l'importance du sujet sur la scène internationale et plus particulièrement de l'intérêt japonais à structurer la collaboration sur cette question.

## 1. Principaux dialogues politiques du Japon

### a. Le développement des partenariats internationaux du Japon

Le Japon a entamé un certain nombre de consultations bilatérales ou multilatérales avec des gouvernements ou institutions étrangères[6263]. Les objectifs du Japon sont multiples :

Une relation forcément privilégiée avec les Etats-Unis

Les Etats-Unis, étant donné leur importance dans le paysage de la défense japonaise, bénéficient d'une position de force pour tout ce qui est lié à la cybersécurité.
Le Japon s'appuie sur l'expertise américaine pour améliorer ses capacités intrinsèques. C'est l'un des objectifs japonais principal pour son **dialogue politique avec les Etats-Unis** lancé en mai 2013 (dont le pré-requis était la signature d'un accord d'échanges d'information sur les cyber-attaques entre le MIC et le *Department of Homeland Security*, effectif depuis mars 2012).
Ainsi on constate l'omniprésence américaine sur le sujet, tant au niveau politique qu'économique et technologique[64].

Quatre réunions du dialogue politique Japon-Etats-Unis ont déjà eu lieu[65], avec comme principaux thèmes[66] :

[61] http://www.japannewsroom.com/wp-content/uploads/2016/05/Joint-Declaration-by-G7-ICT-Ministers.pdf

[62] http://www.mofa.go.jp/policy/page18e_000015.html

[63] http://www.mofa.go.jp/mofaj/annai/page5_000250.html

[64] https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf

[65] http://www.mofa.go.jp/press/release/press4e_001218.html

[66] http://www.state.gov/r/pa/prs/ps/2016/07/260572.htm

- Cybersecurité des infrastructures critiques
- Capacity building à l'international
- Partage de l'information et de l'intelligence cyber
- Coopération militaire sur la cybersécurité
- Cybercrime
- Problèmes de sécurité globaux soulevés par l'espace cyber

Les participants au dialogue américano-japonais en cyber sont :

- *U.S. Department of State*
- *National Security Council*
- *Department of State*
- *Department of Homeland Security*
- *Department of Justice*
- *Department of Defense*
- *Department of Commerce*

Autres dialogues internationaux

Un des objectifs principaux des **dialogues politiques cyber** que les autorités japonaises cherchent à mettre progressivement en place avec leurs partenaires privilégiés, est de favoriser la convergence de vues sur l'élaboration d'un cadre international et l'adoption de mesures de confiance.

Le Japon, qui a activement participé au Groupe des experts gouvernementaux (GGE) sur la cybersécurité de 2012 à 2013, défend le principe de la **liberté de circulation de l'information** et la formulation de **règles internationales fondées sur les normes existantes** (en opposition aux positions défendues par la Chine et la Russie). Il souhaite le développement d'un cadre approprié de coopération internationale facilitant les échanges d'information et permettant d'apporter des réponses appropriées aux menaces identifiées. En matière de cybercriminalité, il promeut la Convention de Budapest, qu'il a lui-même ratifié fin 2013.

En dehors des Etats-Unis, le dialogue cyber le plus développé à ce stade par le Japon concerne le **Royaume-Uni** (lancé en juin 2012) et couvre un large spectre (y compris le partage d'expertise en matière de protection des systèmes d'information lors de l'organisation de grands événements comme les Jeux Olympiques).
Le Royaume-Uni bénéficie de l'expérience des Jeux Olympiques de Londres en 2012, réputés pour avoir été un succès du point de vue de la maîtrise de la sécurité informatique.

En effet, durant les jeux de 2012, approximativement 200 millions d'accès malveillants et 11000 demandes d'accès par seconde via des attaques de déni de service (DDos) sur le site officiel des Jeux ont été détectés.

A titre d'exemple, ayant anticipé une cyberattaque prévue sur le système de contrôle de gestion de l'alimentation électrique du stade où devait avoir lieu la cérémonie d'ouverture, l'opérateur en charge a pu passer le système de contrôle d'opération réseau en mode manuel. La collaboration scientifique entre le Royaume-Uni et le Japon est également très active, avec notamment un accord entre plusieurs universités britanniques et le NICT.[67]

Un autre partenaire important du Japon est **Israël**, notamment pour la R&D (ce qui a constitué le premier accord entre gouvernements de ce type pour le Japon[68]), la formation des professionnels japonais[69] et le développement des partenariats industriels[70], notamment dans l'optique des jeux olympiques de 2020 (des sociétés israéliennes impliquées dans des jeux olympiques antérieurs viendront prêter main forte aux autorités japonaises)[71]. Les questions de défense et de cybercrime font aussi partie des sujets évoqués[72].
Un dialogue politique bilatéral, dont la seconde édition a eu lieu en juin 2016, structure la relation entre ces deux pays[73]. Il est à noter également que la cybersécurité occupe également une place importante également dans le dialogue économique entre le Japon et Israël[74].

Un dialogue régulier a également été mis en place avec l'**Estonie** (qui accueille sur son territoire un Centre d'excellence de cyberdéfense), pays pionner dans l'adoption des technologies numériques dans le monde.

Une première session d'un dialogue bilatéral avec l'**Inde** s'est également tenue en 2012. Des discussions cyber entre gouvernements japonais et **allemands** ont également été entamés (2016).

Enfin, le « 2+2 » ministériel organisé avec la **Russie** en octobre 2013 s'est achevé par l'annonce d'une coopération bilatérale dans le domaine cyber.
Le Japon a également initié en 2015 un dialogue politique avec **l'Australie**[75], membre des « 5 eyes » (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) et proche de l'ASEAN, et qui a donc une influence potentielle importante sur le sujet.

---

[67] http://www.gov.uk/government/world-location-news/uk-universities-sign-agreement-with-nict-on-cyber-security-research

[68] http://www.matimop.org.il/japan_agreement.html

[69] http://www.timesofisrael.com/israeli-solution-to-train-japanese-cyber-warriors/

[70] http://www.geektime.com/2016/01/31/japan-comes-looking-for-israeli-cyber-security-startups/

[71] http://www.globes.co.il/en/article-7-israeli-tech-brands-unite-to-break-into-japan-1001095257

[72] http://thediplomat.com/2015/01/japan-and-israel-to-work-together-in-cyberspace/

[73] http://www.mofa.go.jp/me_a/me1/il/page22e_000777.html

[74] http://www.meti.go.jp/english/press/2016/0613_03.html

[75] http://dfat.gov.au/news/media-releases/Pages/inaugural-australia-japan-cyber-policy-dialogue.aspx

Un dialogue avec l'**Union Européenne** a été mis en place en 2014[76], notamment pour échanger sur les normes mises en place dans les pays membres, ainsi que les questions de cybercrime et de renforcement des capacités.
Le Japon investigue par ailleurs avec l'**OTAN** comment les deux entités pourraient travailler ensemble[77].

Enfin, le Japon a établi un dialogue trilatéral sur les questions cyber avec la Chine et la Corée du Sud[78], avec lesquels les relations diplomatiques sont parfois tendues.

Efforts d'influence du Japon en matière de renforcement des capacités (« *capacity-building* ») dans des pays tiers.

Le Japon concentre actuellement ses efforts vers deux régions :

- **Les pays de l'ASEAN**, au travers d'initiatives de développement des ressources humaines et de projets spécifique de partage des données sur la supervision du trafic Internet (TSUBAME) ou de coopération technique (JASPER), soutenus par des dialogues politiques réguliers (*ASEAN-Japan Ministerial Meeting on Cybersecurity Cooperation, ASEAN-Japan Information Security Policy Meeting, ASEAN-Japan Ministerial Meeting on Transnational Crime*) ;

Les deux principaux projets de collaboration sont :
- La collaboration technologique (JASPER - Japan-ASEAN Security Partnership))
    - PRACTICE (5 pays en avril 2015)
    - DAEDALUS (5 pays en avril 2015
- Le renforcement conjoint des capacités (« capacity building »)

Le MIC a également organisé plusieurs colloques sur la collaboration avec l'ASEAN :
- Octobre 2014 : 7ème rencontres Japon-ASEAN sur la politique cybersécurité -Tokyo (pays de l'ASEAN participants : Brunei, Cambodge, Indonésie, Laos, Malaysie, Myanmar, Philippines, Singapour, Thaïlande, Vietnam)
- Octobre 2014 : 5ème workshop FAI - Philippines
- May 2014 : APT forum sur la cybersécurité - Mongolie
- APEC
- ITU-T

- **Les pays africains**, en participant à l'établissement de centres d'alerte et de réaction aux attaques informatiques (CSIRT) et en organisant des sessions de formation régionales

[76] http://www.mofa.go.jp/press/release/press4e_000447.html

[77] http://www.nato.int/cps/en/natolive/news_102417.htm?selectedLocale=en

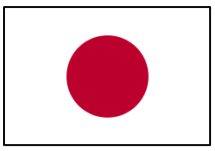
[78] http://www.mofa.go.jp/press/release/press4e_000892.html

(Rwanda, Afrique du Sud, Tanzanie, Cameroun, Gambie et Soudan au cours de ces trois dernières années).

### b. Dialogue politique franco-japonais

La France a également initié un certain nombre de dialogues politiques sur les questions cyber avec des partenaires internationaux majeurs, notamment avec les Etats-Unis, le Royaume-Uni, l'Allemagne, la Russie, la Chine, l'Inde, etc.

**Entre la France et le Japon, un dialogue politique bilatéral,** dont la première rencontre a eu lieu en décembre 2014 à Paris est en cours. Les acteurs impliqués dans ce dialogue sont :

| **FRANCE** | **JAPON** |
|---|---|
|  |  |
| Ministère des Affaires Etrangères et du Développement International (MAEDI)<br>ANSSI<br>Ministère de l'Intérieur<br>Ministère de la Défense | Ministry of Foreign Affairs of Japan (MOFA)<br>NISC<br>NPA (National Police Agency)<br>National Security Secretariat (NSS)<br>CIRO (Cabinet Intelligence and Research Office[79], Naichō - 内調)<br>Ministry of Defense<br>METI (Ministry of Economy, Trade and Industry)<br>MIC (Ministry of Internal Affairs and Communications) |

Ce dialogue a pour objectifs principaux d'atteindre une meilleure compréhension des organisations et politiques respectives et d'échanger sur des thèmes divers : évaluation des menaces, combat contre la cybercriminalité, règlementation de l'espace cyber à l'échelle internationale.

La seconde rencontre du dialogue franco-japonais a eu lieu en début d'année 2016 à Tokyo. La troisième édition devrait avoir lieu en début d'année 2017 à Paris.

[79] Agence d'Intelligence japonaise

Parmi les thèmes prometteurs, peuvent être cités les suivants :

- La formation : le Japon a souligné ses difficultés dans le domaine, à la fois pour les jeunes diplômés comme pour la formation des personnels à ces nouvelles problématiques
- La coopération pour le *capacity building* en pays tiers (le Japon a initié des initiatives en Asie du Sud-Est, tandis que la France a des relations privilégiées en Afrique)
- La protection des infrastructures vitales,
- L'échange d'expérience dans le cadre des événements de grande envergure (Jeux Olympiques, COP21, Euro de football …)
- La cyberdéfense

Par ailleurs, lors de la deuxième réunion du dialogue politique à Tokyo, un état d'avancement de l'initiative scientifique franco-japonaise lancée en avril 2016 a été présenté devant les décideurs politiques membres de cette initiative.

## 2. Collaborations scientifiques avec le Japon

### a. Les partenaires majeurs du Japon

Comme mentionné auparavant, les Etats-Unis jouent un rôle majeur dans le paysage de la cybersécurité japonaise. A ce titre, les évènements communs sont nombreux.

L'initiative de ces évènements est souvent organisée par le département commercial de l'Ambassade des Etats-Unis au Japon, ainsi que la fondation Sasakawa pour la paix (*Sasakawa Peace foundation*).

Quelques évènements notables ont été organisés en partenariat ces derniers mois :

- *Okinawa cybersecurity C3 conference 2015* [80](organisée par le *World economic forum* et le *Cabinet Office* japonais) :
- http://www8.cao.go.jp/okinawa/3/cyber3/press_release_en0910.pdf
- Spotlight 2020 : http://spotlight2020.jp/
- Volet cybersécurité US lors du salon CEATECH
- *International Cybersecurity Symposium* avec l'Université de Keio et l'Ambassade du Royaume-Uni – Critical Infrastructure Protection towards 2020 Tokyo – https://www.keio.ac.jp/en/news/2016/160304-2.html

Le pouvoir de lobby américain est très influent sur les institutions japonaises, de par leurs liens historiques en matière de défense.

### b. Les partenariats entre l'Union Européenne et le Japon

Les accords suivants ont été mis en place avec les pays d'Europe :

| **France** |
|---|
| Collaboration dans le domaine de la cybersécurité entre le NICT (*National Institute of Information and Communications Technology*) et Inria. Un accord a été signé le 21 novembre 2014 et des échanges de données sur l'Internet profond (Darknet) ont alors été initiés. |
| **Royaume-Uni** |
| Collaboration dans le domaine de la cybersécurité entre le NICT et trois Universités du Royaume-Uni (Imperial College of Science, Technology and Medicine, Université du Lancaster et Université du Queens à Belfast). Un accord a été signé le 9 février 2015 et un premier workshop « UK-Japon » a |

[80] http://www8.cao.go.jp/okinawa/3/cyber3/press_release_en1030.pdf

| |
|---|
| été organisé à la suite. |
| **Pays-Bas** |
| Collaboration sur le projet PRACTICE avec l'Université de Technologie de Delft. Des échanges de données sur l'Internet profond (Darknet) ont débuté le 18 février 2015. |

### c. Collaboration scientifique entre la France et le Japon

Dans le cadre du dialogue politique franco-japonais sur la cybersécurité, l'Ambassade de France au Japon a organisé, conjointement avec le NICT, l'Université Keio, Inria et le CNRS, un événement de trois jours dédié à la cybersécurité, du 1er au 3 Avril 2015 à Tōkyō. L'objectif de cet événement était de développer les composantes scientifique et technologique de ce dialogue politique.

Une quarantaine de présentations, alternant intervenants français et japonais issus de la recherche publique et privée, ont permis de couvrir l'ensemble des axes clés de recherche liés à la cybersécurité : sécurité des réseaux, sécurité des logiciels et des systèmes, sécurité dans le cloud, internet des objets, gestion des attaques, cryptographie, méthodes formelles et vérifications et protection des données privées.

Cet événement a réuni plus de 120 participants dont de nombreux représentants d'entreprises (Thales, Quarkslab, Safran/Morpho, Oberthur, Orange Labs, NTT, Hitachi, KDDI, Telecom ISAC, FFRI, TrendMicro, NEC, ASOK), ainsi que des représentants du gouvernement japonais (Ministère des Affaires Intérieures et Communications, Ministère des affaires étrangères, Agence nationale de police japonaise, Ministère de la défense, Ministère de l'économie, du commerce et de l'industrie).


Figure 24 : premier évènement scientifique franco-japonais sur la cybersécurité à Tokyo

Un **comité de pilotage** global a été établi pour le suivi de la collaboration et sur l'identification de schémas de financement.

8 thématiques scientifiques prioritaires pour la collaboration ont été mises en avant, pour lesquelles **8 groupes de travail** ont été lancés, chacun étant animé par deux pilotes, français et japonais, désignés lors du séminaire. Ces groupes de travail sont chargés de l'animation de la coopération sur leur thème et du suivi de son avancée:

- WG1: <Méthodes formelles> : protocoles cryptographiques, vérification, protection des données privées par méthodes formelles
- WG2 <Cryptographie> Cryptographie à base de réseaux euclidiens and cryptographie post-quantique
- WG3 <Analyse des incidents et des malware > récoltes d'information à partir de capteurs (en particulier dans le *darknet*) et échanges d'information pour l'analyse des cyberattaques et des malware
- WG4 <Sécurité des systèmes et de l'IoT> contremesures contre les attaques par canaux auxiliaires
- WG5 <Données privées> Technologies d'assainissement, de généralisation et Data Mining pour la protection des données privées
- WG6 <Sécurité ICS/ITS > Sécurité des systèmes de contrôle industriels et des systèmes de transports intelligents
- WG7 <Gestion de crise>
- WG8 <Réseaux, sécurité des réseaux, mesures> Virtualisation, sécurité SDN (Software Defined Networks), dont la mesure de la performance et de l'efficacité en termes de sécurité

L'ensemble de ces groupes est piloté par un comité de pilotage:

| **JAPON** | **FRANCE** |
|---|---|
| • Koji Nakao (NICT)<br>• Mitsuhiro Okada (Keio University)<br>• Jun Murai (Keio University) | • Claude Kirchner (Inria)<br>• Helene Kirchner (Inria)<br>• Phong Nguyen (CNRS & Inria)<br>• Marc-Olivier Killijian (CNRS) |

**Détails des groupes de travail**

Groupe de travail 1 : Méthodes formelles

Objet : Vérification de protocoles cryptographiques / données privées par méthodes formelles

Coordinateurs :

- Georgei Banev (Inria)
- Mitsuhiro Okada (Université de Keio)

Membres :

- Japon: Mitsuhiro Okada (Keio University), Yusuke Kawamoto (AIST-Tsukuba), Reynald Affeldt (AIST-Tsukuba), Tachio Terauchi (JAIST)
- France: Hubert Comon (ENS-Cachan, CNRS), Catuscia Palamidessi (INRIA Saclay and LIX), Gergei Bana (INRIA Paris-Rocquencourt), Pascal Lafourcade (Université d'Auvergne (Clermont 1)), Kostas Chatzikokolakis (INRIA Saclay and LIX), Gilles Grimaud (Université des Sciences et Technologies de Lille)

Thèmes de recherche :

Méthode formelle : discipline visant à modéliser un attaquant de manière aussi réaliste que possible d'une façon formelle et précisément définie. Il s'agit ensuite pour tout protocole donné, soit de prouver qu'il n'y a pas d'attaque possible et, si ce n'est pas le cas, d'identifier les attaques possibles.

Cette méthode consiste à développer des programmes de vérifications automatiques.

Principaux efforts de recherche :

1. Vérification de complexité théorique (appelée computationnelle)
2. Flot d'information quantitatif, confidentialité différentielle
3. Techniques de vérification de protocoles de sécurité par preuves en Coq
4. Intégration des technologies 1.2.3.

Site internet du groupe : http://prosecco.gforge.inria.fr/personal/gebana/Site/Franco-Japanese-WG1.html

Groupe de travail 2 : Cryptographie

Cryptographie : Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée (ISO 7498-2).

Coordinateurs :

- Phong Nguyen (Inria)
- Shiho Moriai (NICT)

Membres :

- France: Pierre-Alain Fouque (Univ. Rennes), Adeline Langlois (CNRS), Guenael Renault (UPMC).
- Japan: Yoshinori Aono and Naoyuki Shinohara (NICT), Noboru Kunihiro (Univ. Tokyo), Tsuyoshi Takagi (Kyushu Univ.), Mehdi Tibouchi (NTT).

Thèmes de recherche :

Cryptographie post-quantique, cryptographie à base de réseau euclidien.

Groupe de travail 3 : Events and Malware Analysis

Coordinateurs : Marion Jean-Yves, Dai Inoue

Thèmes de recherche :

- les sondes darknet et les moteurs de visualisation de NICTER (l'outil du NICT) ont été mis en place au LHS CNRS-INRIA-Université de Lorraine
- le NICT, le CNRS, l'Inria et l'Université de Lorraine échangent au sujet du trafic monitoré par chacune des organisations.
- L'Université de Lorraine et le JAIST à Kanagawa ont signé un MoU le 7 décembre 2015 à Nancy, sur l'analyse des logiciels malveillants. Un projet CNRS-JSPS a également été soumis.

Groupe de travail 4 : System Security and IoT security

Coordinateurs : Lanet Jean-Louis (Inria), Shinsaku Kiyomoto (KDDI labs)

Membres :

- France: Lanet Jean-Louis + {Telecom Sud Paris, Univ-Lille, Inria, Telecom Paristech, Secure-IC, Cnam, Laas if more activities}
- Japon: Shinsaku Kiyomoto (KDDI labs) and Kazukuni Kobara (AIST)

Thèmes de recherche :

- Environnement d'exécution sécurisé pour l'Internet des Objets (IoT). Les métriques utilisées pour la mesure de la performance sont la taille du code, les temps de transaction, l'utilisation mémoire, la taille des données et les coûts d'implémentation
    - Lightweight software obfuscation
    - Software tamper-resistant techniques
    - Management (and hiding) of secret keys
    - Side-channel resistance (leakage resilience)
    - Secure updating of IoT modules
- Architecture sécurisée pour les plateformes IoT. Les métriques utilisées pour la mesure de la performance sont l'évolutivité, le taux de détection, la standardisation, les indicateurs de protection des données privées et les coûts estimés de gestion
    - Efficient AAA framework for huge number of devices

- Privacy policy management
- Malware detection on IoT platform
- Traffic analysis and malicious device detection
- Secure updating of devices, programs, data, cryptographic keys and modules.

Groupe de travail 5 : Privacy

Coordinateurs : Sebastien Gambs (Université de. Rennes et Inria); Hiro Kikuchi

- France
  - Sebastien Gambs (U. Rennes et Inria)
  - Daniel le Metayer (Inria)
  - Benjamin Nguyen (INSA)
  - Jacques Traore (Orange Labs)
  - Pascal Paillier (Cryptoexperts)
  - Marc-Olivier Killijian (CNRS)
  - Kevin Huguenin (CNRS)
- Japon
  - Hiroaki Kikuchi (Meiji University)
  - Hiroshi Nakagawa, Univ. of Tokyo
  - Hiromi Arai, Univ. of Tokyo
  - Masayuki Terada, NTT Docomo
  - Kazue Sako, NEC
  - Jun Sakuma, Univ. of Tsukuba
  - Ryo Nojima, NICT
  - Shiho Moriai, NICT

Thèmes de recherche :

- Technologies d'assainissement, généralisation et data mining pour la préservation des données privées.
- Projet d'organiser une compétition internationale d'assainissement et d'anonymisation des données, sur le modèle de la conférence organisée au Japon[81] par l'Université de Meiji, NTT, Fujitsu et Nifty.

Groupe de travail 6 : ICS/ITS Security (Intelligent Control System/ Intelligent Transportation System)

[81] https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&page_id=13&block_id=8&item_id=146842&item_no=1

Coordinateurs : Assia Tria (CEA) et Koji Nakao (NICT, KDDI)

Thèmes potentiels de collaboration :

- ICS : protection des infrastructures ICS, supervision de la sécurité des ICS, gestion de l'identité à travers les différents appareils de l'ICS, réponses en cas d'incident, exploitation de systèmes embarqués, déploiement de honeypot (« pot de miel », leurre) pour l'ICS
- ITS : point d'ancrage de confiance matériel pour la sécurisation des voitures connectées, sécurisation des véhicules autonomes, prévention et détection d'intrusions, mises à jour sécurisées pour les logiciels embarqués, architecture sécurisée et outils de validation pour les réseaux de véhicules interconnectés.

Groupe de travail 7 : WG7: Crisis Management

Coordinateurs  Claude Kirchner (Inria), Koji Nakao (NICT, KDDI)

Thèmes potentiels de collaboration : mise en place de mesures d'action en cas d'attaque et mitigation des dégâts.

Groupe de travail 8 : Network Virtualization, security, management

Coordinateurs : T. Silverston (Univ. Nancy), Prof. Sekiya (Todai / WIDE)

Participants

- Discussions avec des membres du projet WIDE et en particulier Prof. Tsukada, Sekiya et Tazeki (U. Tokyo / WIDE)
- Etudiant doctorant de U. Tokyo va venir effectuer un PhD au LORIA (Nancy)

- Objectifs
  - Projets bilatéraux (équipe Inria, etc)
  - Kakenhi au Japon (sur la virtualisation NDN et les cas d'utilisation avec l'IoT) avec le Prof. Tsukada (Todai / WIDE) (NDN: Named Data Network)

Thèmes de recherche :

- NFV (*Network Function Virtualisation*), sécurité SDN (*Software Defined Networks*), incluant la gestion de la sécurité et des outils de mesures
- Doctor Project (http://doctor-project.org): NDN virtual test-bed. Prochaines étapes: outils de supervisions et de sécurité pour NDN virtuel et IETF
- Discussions avec le Prof. Asaeda (NICT) pour des test-beds NDN

Un second séminaire s'est tenu en France, à Rennes, du 21 au 23 septembre 2016, en partenariat avec le PEC (pôle d'excellence cyber Bretagne). Ce workshop a été l'occasion de faire un état d'avancement des 8 groupes de travail et a également donné lieu à plusieurs conférences invitées, notamment par des acteurs industriels français. Un programme de visite a également été organisé, notamment du Laboratoire de Haute Sécurité du PEC, ou de l'institut B-Com.

Compte tenu du succès de ce second workshop, **la tenue d'une troisième édition a été décidée et fixée aux 24 et 25 avril 2017**, à l'Université Keio, à Tokyo.

**Japanese-French joint Laboratory for Informatics (JFLI), un outil pour la collaboration**[82]

Le JFLI, unité mixte de recherche franco-japonaise en informatique dont le nouveau directeur (Phong, Nguyen) est spécialisé en cryptographie, a notamment été présenté comme une structure fédératrice clé pour renforcer la collaboration.

Le JFLI a été créé en janvier 2009 en tant que LIA (Laboratoire International Associé), avant d'être labellisé en 2012 UMI (UMI - Unité Mixte Internationale)

Le JFLI collabore en France sur la cybersécurité avec un certain nombre d'acteurs comme LIP6 (Paris), LIAFA (Paris), STMS (Paris), LRI (Paris), LIFL (Lille), Lab. Physique (Lyon), LaBRI (Bordeaux), IRIT (Toulouse), LCTI (Paris), LORIA (Nancy), IRISA (Rennes), Icube (Strasbourg)

Le JLFI peut être un hub pour la collaboration bilatérale, à travers l'accueil de membres des groupes de travail pour des séjours courts ou plus long ou encore l'organisation d'évènements thématiques.

Le JFLI possède également un réseau de professeurs japonais « partenaires » parmi les institutions affiliées, potentiellement superviseurs de projets ou encadrants d'étudiants/chercheurs.

Les thèmes de recherche du JFLI (d'autres thèmes de recherche peuvent être ajoutés) sont :

- Réseaux de nouvelle generation
    - Modélisation et mesure des réseaux, réseaux mobiles, réseaux ad hoc
- Calcul haute performance
    - Paradigmes de programmation et langages pour les supercalculateurs, algorithmes méthodes itératives et auto-ajustement, cloud computing, gestion de grandes quantités de données
- Logiciel, modèles de programmation et méthodes formelles
    - Vérification logicielle, méthodes formelles, sécurité de l'information
- Image et multimédia

[82] http://jfli.cnrs.fr

  - Réalité virtuelle, interfaces et interaction, analyse du contenu multimédia et récupération de données et du contenu numérique
- Informatique quantique
  - Cryptographie et communications quantiques, algorithmes quantiques

Plus d'informations sur le JFLI :

- Directeurs : K. Nemoto (NII) et P. Nguyen (Inria)
- 7 chercheurs français au Japon
- 10 professeurs japonais partenaires
- Le JFLI est éligible aux
  - Aux financements français et européen (en tant qu'UMI du CNRS)
  - Financements japonais : les chercheurs français travaillant des institutions japonais peuvent postuler
- Le JFLI gère un budget à la fois en France et au Japon
- Un laboratoire conjoint comme le JFLI simplifie les collaborations
  - le JFLI peut recevoir des chercheurs français sur trois différents sites (U. Tokyo, U. Keio et NII) et peut s'occuper des formalités administratives (visa, etc.)
  - le JFLI peut accueillir des chercheurs Inria/CNRS pour des séjours longs (1-2 ans) ainsi que des professeurs d'universités en année sabatique

Partenaires du JFLI :

| **JAPON**<br><br>3 partenaires | **FRANCE**<br><br>3 partenaires |
|---|---|
| NII 国立情報学研究所 National Institute of Informatics ; 慶應義塾 Keio University ; 東京大学 THE UNIVERSITY OF TOKYO | cnrs ; Inria ; UPMC SORBONNE UNIVERSITÉS |

# Conclusions et futures actions

La France et le Japon partagent des menaces communes dans le domaine de la cybersécurité, mais également des valeurs communes pour les combattre (protection de la confidentialité des données, partage d'information..). Dans le cadre du dialogue politique cyber lancé en 2014 entre les deux pays, et réunissant les différents acteurs du domaine, une relation de confiance s'est engagée et plusieurs axes clés de collaboration ont été identifiés (mise en place d'un framework pour l'échange de données sur les malware, collaboration sur la sécurité des grands événements, comme les Jeux Olympiques et Paralympiques de 2020, basée sur l'expérience française de l'Euro de football, ou de la COP21, ou encore dans le domaine de la formation ou du *capacity building* en pays tiers).

La science et la technologie est un volet de la coopération franco-japonaise qui peut permettre de soutenir et alimenter ce dialogue politique à plusieurs égards : d'une part, pour réunir les meilleures compétences afin de mettre au point des solutions technologiques face aux menaces cyber et, d'autre part, pour que l'expertise des chercheurs de ce domaine très technique et évolutif soit mise à disposition des décideurs politiques. Suite à un premier événement organisé par l'ambassade de France à Tokyo en avril 2015, une initiative scientifique franco-japonaise réunissant les acteurs académiques, gouvernementaux et privés a été lancée. Cette collaboration à la fois très dynamique et structurée s'inscrit sur le long terme, comme le montre la tenue du 3ème workshop à Tokyo en avril 2017 et le lancement de plusieurs projets soutenus conjointement par les institutions françaises et japonaises. Des échanges entre cette initiative scientifique et le dialogue politique cyber ont été initiés lors de la deuxième réunion du dialogue politique et devraient se poursuivre à l'occasion des prochaines réunions.

Plusieurs axes de coopération gagneraient à être renforcés, notamment la sécurité matérielle, la sécurité de l'IoT, celle des véhicules autonomes, la formation ou encore la gestion des infrastructures critiques, en particulier lors des évènements de grande ampleur (comme les jeux olympiques). L'utilisation de l'intelligence artificielle (*Deep learning*) pour la cybersécurité est également un nouveau sujet à très fort potentiel.