CYDEF2019 Session5

In the Ara of Cyber-attacks Nations Manipulate - National Cyber Defense and Industry -

Moderator

Masaya Norifusa, Cyber Risk Intelligence Center (CRIC)

Panelist

Jun Goto, NEC Corporation

Chikara Nakama, CISCO Systems

Prof. Chris Demchak, US Naval War Collage

Dr. Sandro Gaycken, DSI Berlin (ESMT Berlin)

Positioning

- 企業/産業側から見て、サイバー攻撃/戦争と国防に課題を提議する
- 日本の特徴を理解し、日本ですべきこと、できることを議論する
- 企業と国防の間にある隠れた接点を洗い出す
- 欧米の先行事例を参考にしたい

- With viewpoints of Industries, Cyber-attack(Industry word)/Cyber-war(Defense word) problems to be solved are pointed out
- By understanding Japanese specific characteristics, items should be challenged and/or could be implemented are discussed
- Hidden X-points between Industries and National Defense are dug out
- Referring advanced examples at EU and US

Problems

- 国家がサイバー攻撃に関与すると、高度で執拗な攻撃が加速、増加
- 統制されて成功確率は高い
- サイバー軍同士の攻防にならず、企業が攻撃を受け大きな被害を出す
- 被害は企業の金融資産、知的資産、デジタル資産、市場ステータスの喪失など
- 一企業で防げない
- 企業は弱体化し、市場から撤退
- 国力（経済力、技術力）の弱体化

- Cyber-attacks a Nation manipulates accelerate frequency, speed, and persistence
- Well-organized and more successes
- No battles between Cyber forces, and Industries become victims
- Damages are financial, intellectual, and digital assets stolen, that result in market loss
- Almost impossible to defend alone
- Eventually leaving from the market
- Down of the competence of Japan nation

Motivation

- 日本の力は経済力と技術力、これを支えているのは大中小何万社という企業の生産活動
- 美しい国土は残ったが、企業活動と個人の生活を失い国力が弱まった、という事態は避けたい
- 一企業で解決しない、いっしょに取り組むなら
  - 産業横断の企業間協力で？
  - 警察組織と？
  - 防衛組織と？
  - 全てが必要？

- Competence of Japan is economy and technology, grown by enormous skillful production activities by tens of thousands of companies
- Beautiful land remains as today, but companies and personal lives are gone, is NOT acceptable future for Japanese
- Who should work with together to resolve problems:
  - Cross industries?
  - Law enforcement organizations?
  - Defense organizations?
  - All of them?

Start Line

- 「日本の」資産を守って国力を維持するのだから、まずサイバー攻撃への防御に関わる日本固有の状況を理解する
- To maintain and enhance the current (economical and technological) strength of Japan, to protect indispensable assets which are not protected enough and located in accessible spaces in industries and academies, first we start to understand important cybersecurity-related characteristics specific to Japan.

Japanese Characteristics (1)

- 雇用システムが独特。サイバー人材へと育成しやすいIT学生は、卒業時に企業に就職しほとんど転職しない
- 大手ICT企業に、日本のIT人材の過半数がいて、そこで成長する
- 他企業は大手でも、IT人材の確保、サイバー人材への育成は困難
- 企業従事者は、「戦争」「有事」への意識、認識は薄い
- 「サイバー攻撃」は身近でも、「サイバー戦争」は自分のことではない、中身が変わらなくても

- Unique employment system. Graduate students, having talent to be cybersecurity assets, join in a company and keep staying for long
- Large ICT companies maintain more than half of all IT engineers in Japan
- Large companies other than ICT do not employ and grow IT engineers, and therefore cybersecurity assets
- Words of War and Emergency do not appear in a daily company life
- Cyber-attack has been “MY” issue, but Cyber-war is someone’s issue

Japanese Characteristics (2)

- その結果、多くの組織でサイバー人材候補の獲得、専門家への育成は、極めて困難
- 雇用システムは変わりつつあるが、サイバー攻撃への対応が必要なこの先５年の間に大きな変化はない
- 日本には多くの優秀なIT人材がおり、優秀なサイバー人材になる力も備えているのに、必要とする組織でこれら人材を獲得できない、という現状をどう打開してゆけるか

- As result, almost all organizations can not acquire and maintain cybersecurity assets, and almost non are grown in-house
- The current employment system is being broken, but in the next 5 years, change will be still small
- A lot of excellent IT engineers are in Japan, who could be excellent cybersecurity assets, however organizations will need them are always hard to get and grow them

Keep in Mind until End of the Session

- 「日本の国力」を守れる規模の有能なサイバー防衛組織は、人材を維持できず難しいのではないか。しかし、不可欠なので、ならば、どうすればいいのだろうか
- 「日本の国力」を維持するために守るべき資産がたくさんある。これら資産は守り抜かなければ意味がない。「守り抜く」という強い意思を誰が共有しないといけないのか

- It looks difficult to maintain sufficient scale of talented cyber defense teams to be able to protect the power of Japan, because of difficulty of collecting talented cybersecurity human assets. However, it is must. So, then?
- To maintain the power of Japan, there are plenty of valuable assets to be protected. Protecting them until end is must. Who should share this strong will?

Notes

- 16:30-18:00
- パネリストへの「質問」は最後にまとめて受け付ける
- 各お題で、パネリストに回答してもらった後、会場からも1-2名、別の経験や事例を「補足」する機会を設けたい
- 全員参加でディスカッションしたい

- 16:30-18:00
- Questions to the panelists will be arranged at end of the panel. However, during the discussion, after panelist expressed opinions, it may be arranged an opportunity that 1 audience shows additional facts, difference experiences, and beneficial suggestion, to supplement the discussion.
- Discussion by all participation in the room

Discussion (1)

各パネリスト導入プレゼン

- 後藤淳氏、NEC
  1990年代初めから続けてきた情報セキュリティ管理とサイバー攻撃への取り組み
- 仲間力氏、CISCOシステムズ

- クリス・デムチャク博士、米海軍大学（右記）
- サンドロ・ガイチェン博士、DSIベルリン（ESMTベルリン）（右記）

Presentation by panelists

- Jun Goto, NEC
  Challenge of information security and cybersecurity over 25 years to protect the company
- Chikara Nakama, CISCO Systems

- Prof. Chris Demchak, US Naval War Collage
  Systemic Cyber-Economic Defense for a Democratic Minority: a new collective defense mindset and the CORA
- Dr. Sandro Gaycken, DSI Berlin (ESMT Berlin)
  Challenges in setting up national cyber defense capabilities in Europe and the role of the private sector

Discussion (2)

お題1

- 相手は、戦争はしなくても、サイバー攻撃はする。長期戦略で、利益を得つつ相手を弱体化できる。反撃も受けない。価値資産を持つ企業や研究機関を攻撃。こんな状況が定着してしまうのか、あるいはもうしているのか。米国、欧州、日本で違うのか。５年後はどなるのか。

Question1

- The power of Japan is economic strengthen and advanced technology. Industries implement it. Attackers have no-will to arise the War but big-wills to generate benefits. As long-term strategy, they may intend to get instant economical profits and to weaken strength of the opponent nation year by year. Attacks are directed to companies and research organizations that do not have defense. This will come or is already spread?

Discussion (3)

お題2

- サイバー防衛は、技術、経験、陣容、法律、全てこれまでの狭間（無い、足らない、ずれている）に落ち込む。個人戦（個人の力）では負けるので団体戦に持ち込みたい。防衛と企業、どこで組めるか、それぞれに期待したいことは何か。

（その昔、RSAコンファレンスの基調講演で、セキュリティベンダー皆が手を組まないとサイバー攻撃者に勝てない、と言った、けど・・・）

Question2

- Cyber-defense always easily falls into hidden holes of technology, experience, formation, law, and more. Since, at an individual match, defense mostly fails, team match would be alternative for win. For this, what industries and defense organizations expect each other and can do for the other?

Discussion (4)

お題3

- 十分な数と質の人材をサイバー防衛部隊で充足し続けるのは難しい。平時が続く日本では特に難しい。防衛部隊に取り込まず、企業側の優秀なサイバー人材を活用し、かつ企業にもメリットのある協力のあり方はないのか

Question3

- It is difficult to prepare quickly Cyber-defense teams, which are sufficient at both quality and quantity, and maintain them for long, in the defense organization. A lots of small Cyber-defense teams, having few cybersecurity talents, at companies in Japan are subject to defend only each company. For mutual benefits, is there collaboration ways?

Discussion (5)

その他お題

- 欧米での成功・失敗体験から、日本の取り組みにサジェッションしたいこと

Question samples

- Are there advanced examples at EU and US?
- From the experience, suggestion to Japan?

Discussion (6)

最後のお題

- 実行に移さないと何も変わらない。明日から何か一つ実行に移すとしたら、それは何か

Last Question

- Suggest one item to Japan (Gov., Mil., Industries) who better challenge to implement from tomorrow

Closing Notes

Thank you !

Memo for Summary

- Doing collaboration from the Peace status is indispensable
- Not meaning of “one defense unit + one ICT company”, but forming a virtually enough large team for Japan
- Still 90% of companies (medium to small) in Japan are left from the discussion
- Keep discussing, move forward

English

- 日本語

- English

日本語

- 日本語

English

- English