Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2018 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-26-2018

Review of National Cybersecurity Policies

Shigeo Mori
Institute of Information Security, dgs154101@iisec.ac.jp

Atsuhiro Goto
Institute of Information Security, goto@iisec.ac.jp

Review of National Cybersecurity Strategy Case Study: UK

Indicate Submission Type: Research-in-Progress

Shigeo Mori
Graduate School,
Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ku,
Yokohama-city, Kanagawa, Japan
dgs154101@iisec.ac.jp

Atsuhiro Goto
Institute of Information Security

2-14-1 Tsuruya-cho, Kanagawa-ku,
Yokohama-city, Kanagawa, Japan
goto@iisec.ac.jp

Abstract

The damages caused by cyber-attacks are becoming larger, broader and more serious as well as to include monetary losses and losses of lifeline. Some cyber-attacks are arguably suspected to be parts of national campaigns. Under such circumstances, efforts by the private sector are not enough to counteract against cyber-attacks, and the public sector must endeavour to enhance national cybersecurity capacities so that the nation can retain safe and secure life of nationals. We think it very important to ensure that the national cybersecurity strategies are sufficient, appropriate and up-to-dated, so that the national capacities progress towards the right direction at the adequate speed.

Thus, we devised the method to review national cybersecurity strategies and used it to review the UK cybersecurity strategy. The result proved that the carefully formulated national strategies still need review and the method should work.

Keywords: Cybersecurity, National strategy, Capacity Maturity Model

Background

Cyber incidents are reported almost everyday. Although the targets, the attack methods, the damages, the presumed attackers and the presumed objectives are various, the impacts seem to be getting larger, broader and more serious. In October 2017, Yahoo! announced that it'd had 3 billion customer data exfiltrated by cyber-attack (Oath Inc. 2017). In February 2016, Bangladesh Bank, the central bank of Bangladesh, was attacked and had US$ 951 million stolen via SWIFT network (New York Times 2016). In December 2015 and in December 2016, Ukraine experienced wide area power downs due to cyber-attacks (SANS ICS 2016) (SANS ICS 2016). Now cyber-attacks can cause huge impact, monetary damages and even affect daily life of citizens. Some incidents are arguably suspected to be parts of national campaigns (The United States Executive Order 2015).

Under such circumstances, efforts by the private sector including individuals are not enough to counteract against cyber-attacks, and the public sector must endeavour to enhance national cybersecurity capacities so that the nation can retain safe and secure life of nationals.

Tagawa and Hayashi (2017) think it necessary to seek enhancement of the national cybersecurity in every aspect with the combined efforts of the whole country. They also think it should be done by building the proactive national cybersecurity capacities, based on the sustained and private-sector-initiated reactive cybersecurity countermeasures (original in Japanese).

Now that responsibilities of the public sector to enhance national cybersecurity are essential, we think it very important to ensure that the national cybersecurity strategies are sufficient, appropriate and up-to-dated, so that the national capacities progress towards the right direction at the adequate speed. If the strategies are insufficient, inappropriate or out-of-dated, nations' ICTs can be endangered, so is the daily life of the nationals, while the excessive strategies will end up as a waste of taxpayers' money.

There are several trials for cybersecurity benchmarking for nations. Global Cybersecurity Indices announced by ITU (International Telecommunication Union) and the Cybersecurity Capability/Capacity Maturity Models developed by the Global Cyber Security Capacity Centre founded around the Oxford University are the examples of those kind (ITU 2017) (Global Cyber Security Capacity Centre 2014) (Global Cyber Security Capacity Centre 2017). Benchmarking gives us the idea that shows a nation's relative cybersecurity strength among the world. However, as technology, skills of attackers and capacities of other nations develop, a nation must pay a lot of deals to hang onto the pace. Furthermore, if the nation's current benchmarking result is not satisfactory, it must work even harder to surpass the development speed of the others.

Therefore, while benchmarking gives us the important information of the current capacity of the nation, it is just a snapshot and more importantly we need to know whether the nation's cybersecurity capacities are advancing to the desirable level in the coming years. Thus, we point out importance to review the national strategies of cybersecurity capacity enhancement.

Relationship of circumstances, public sectors' responsibilities, benchmarking and review of strategies is shown in the **Figure 1**, and relationship of development speed of nations and attackers, benchmarking and review of strategies is shown in the **Figure 2**.

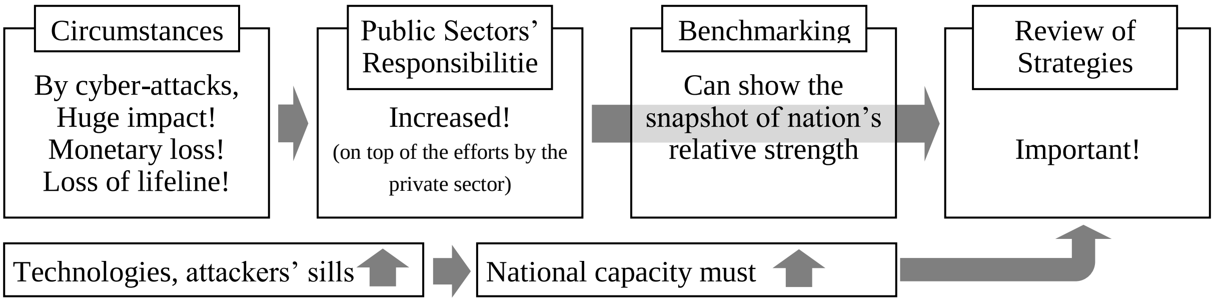
Circumstances
By cyber-attacks, Huge impact! Monetary loss! Loss of lifeline!
Public Sectors' Responsibilitie
Increased!
(on top of the efforts by the private sector)
Benchmarking
Can show the snapshot of nation's relative strength
Review of Strategies
Important!
Technologies, attackers' sills
National capacity must

Figure 1. Circumstances, Responsibilities, Benchmarking & Review of Strategies

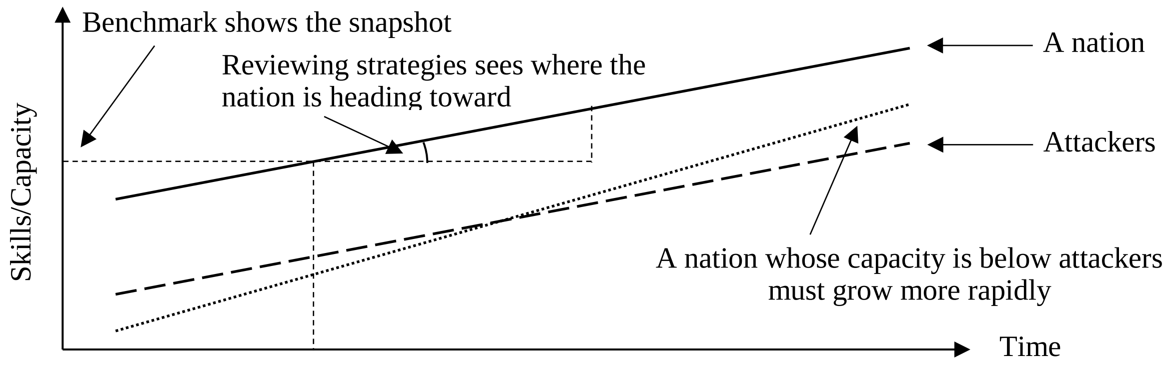
Benchmark shows the snapshot
Reviewing strategies sees where the nation is heading toward
A nation
Attackers
A nation whose capacity is below attackers must grow more rapidly
Skills/Capacity
Time

Figure 2. Development speed of Nations and Attackers, Benchmarking & Review of Strategies

The United Kingdom (hereafter "UK"), where the Global Cyber Security Capacity Centre is located, carried out the official assessment of its cybersecurity capability using the Cybersecurity Capability Maturity Model in 2015 (the result was reported in November 2016) (Global Cyber Security Capacity Centre 2016). In November 2016, the government of UK announced its "National Cyber Security Strategy 2016-2021" (Government of UK 2016). The assessment is assumed to be reflected into the strategy, and the comparison of the two is supposed to show if the cybersecurity strategies are sufficient and appropriate.

Cybersecurity Capability/Capacity Maturity Model

The Global Cyber Security Capacity Centre founded around the Oxford University released the Cybersecurity Capability Maturity Model (hereafter "CSCMM") v1.2 in December 2014 as the first public edition and the Cybersecurity Capacity Maturity Model for Nations Revised Edition (hereafter "CSCMMN") in February 2017.

The Cybersecurity Capability/Capacity Maturity Models are aimed at assisting nations improve their cybersecurity capabilities in a systematic and substantive way.

The Centre considers cybersecurity capacity to comprise the following five 'Dimensions'.

1. Devising cybersecurity policy and strategy
2. Encouraging responsible cybersecurity culture within society
3. Developing cybersecurity knowledge
4. Creating effective legal and regulatory frameworks
5. Controlling risks through standards, organisations and technologies

Each dimension is categorized into several 'Factors', which then are divided into multiple 'Aspects' (in Revised Edition. It was called as 'Categories' in the v1.2). The Revised Edition has 5 dimensions, 24 factors and 53 aspects (v1.2 has 5 dimensions, 20 factors and 47 categories).

The Centre also defined the 5 'Stages' ('Levels' in the v1.2) as the degree of the progress of the nation in relation to a certain aspect of cybersecurity capacity. The 5 stages are 'Start-up', 'Formative', 'Established', 'Strategic' and 'Dynamic'. Each stage has 'Indicators' which describe the steps, actions, or building blocks that are indicative of a specific stage of maturity within a distinct aspect. A Nation must fulfil all indicators within a particular stage to elevate to the next stage.

The relationship of 'Dimension', 'Factor', 'Aspect', 'Stage' and 'Indicator' is shown in the **Figure 3**.

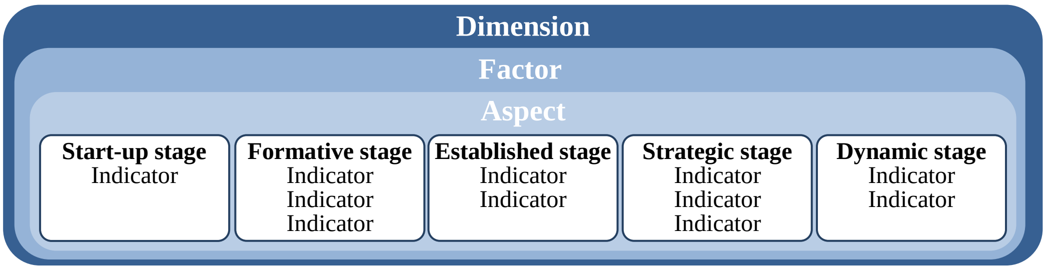

Figure 3. Relationship of Elements in CSCMMN
(produced based on the Cybersecurity Capacity Maturity Model for Nations Revised Edition)

Uganda, Senegal, Bhutan and Kosovo had pilot assessment using v1.2 and the official assessment of the U.K. was done with the same version (Global Cyber Security Capacity Centre 2016) (Global Cyber Security Capacity Centre 2016) (Global Cyber Security Capacity Centre 2015) (Global Cyber Security Capacity Centre 2015) (Global Cyber Security Capacity Centre 2016). Assessment using the Revised Edition may possibly be underway but hasn't been announced yet.

Cyber Security Strategy of the UK

The UK released the National Cyber Security Strategy 2016-2021 in November 2016 and stated in its "Foreword" that 'Much of our prosperity now depends on our ability to secure our technology, data and networks from the many threats we face. Yet cyber-attacks are growing more frequent, sophisticated and damaging when they succeed. So, we are taking decisive action to protect both our economy and the privacy of UK citizens.'

The UK had formerly announced the UK Cyber Security Strategy 2011-2016 (Government of UK 2011) with £860m underpinned for the National Cyber Security Programme. Under the new strategy, the UK 'will invest £1.9 billion in defending our systems and infrastructure, deterring our adversaries, and developing a whole-society capability - from the biggest companies to the individual citizen.'

In the new strategy, the cybersecurity policies are described in the categories - Defend, Deter, Develop and International Action.

The report of assessment using the CSCMM, "Cybersecurity Capacity Review of the United Kingdom", states in its 'Introduction' that the evaluation 'will contribute to the development of the UK National Cybersecurity Strategy 2016–2020.'

Comparing Assessment & Strategy

As mentioned in the "Background", comparison of the assessment and the strategy may reveal sufficiency and appropriateness of the cybersecurity strategy of the UK because the strategy was decided based on the assessment, assuming the CSCMMN which gave the gauge to assessment represents the definitive sufficiency and appropriateness for the desired state of the national cybersecurity.

Comparison, in my research, is done by 'mapping' the national cybersecurity strategies to the CSCMMN and examining if the strategies are laid out adequately based on the result of assessment. 'Mapping' in this case means to find out the indicator(s) of the CSCMMN which an approach is expected to achieve or to contribute achieving. If the strategies (or, the approaches described in the strategies) are sufficient and appropriate, they will sit in the stages next to the stages where the nation currently stands.

For example, if the nation is at 'Established' stage (3rd stage from the lowest) in a particular aspect, the approaches intended to achieve 'Strategic' stage (4th stage) will be adequate, while the approaches for 'Formative' stage (2nd stage) would be questionable. Please refer to the **Figure 4**.

		Start-up	Formative	Established	Strategic	Dynamic
Aspect	Assessment	achieved	achieved	achieved	unachieved	unachieved
	Approaches		###		###	

Questionable

Adequate

Figure 4. Adequate Approaches & Questionable Approaches

When the nation stands at the relatively lower stages, i.e. 'Start-up' or 'Formative' in some aspects, if the nation plans to have no or few approaches to achieve the 'Established' stage or higher, the capacity of the nation in those aspects will remain at the lower stages and become even weaker as the capacities of the others develop. In such cases, the cybersecurity strategy of the nation should be considered insufficient in those aspects. On the other hand, if pretty much proportion of the approaches are concentrated to a few aspects, the approaches need to be examined if there's no duplication of the approaches to realize the same thing, out-of-dated approaches which cannot be terminated by some reasons nor any other inefficient approaches. If any, those approaches should be considered inappropriate. Examples are shown in the **Figure 5**.

		Start-up	Formative	Established	Strategic	Dynamic	
Aspect 1	Assessment	achieved	achieved	unachieved	unachieved	unachieved	
	Approaches	-	some	few	no	no	← Insufficient?
Aspect 2	Assessment	achieved	achieved	achieved	achieved	unachieved	
	Approaches	-	some	many	many	many	← Inappropriate?

Figure 5. (possibly) Insufficient Approaches & (possibly) Inappropriate Approaches

Practical Work of Comparison

Firstly, the cybersecurity approaches described in the National Cyber Security Strategy 2016-2021 must be broken down to the pieces of the practical actions. I call them as the “Action Items”. I extracted 142 action items from the strategy.

Secondly, each action items are mapped on to the CSCMMN, in other words, I sought the indicators which each action item will achieve or contribute to achieve. I call this interconnection as the “Relation”, or “action item A is related to indicator X”. Some action items have two or more relations and I found 307 relations in total.

Next, 307 relations are aggregated by the aspects, then by the factors (upper categorization to the aspect).

Finally, the number of the relations by the factors are compared with the stages that the UK was evaluated to have achieved.

The image of “mapping” is shown in the **Figure 6**.

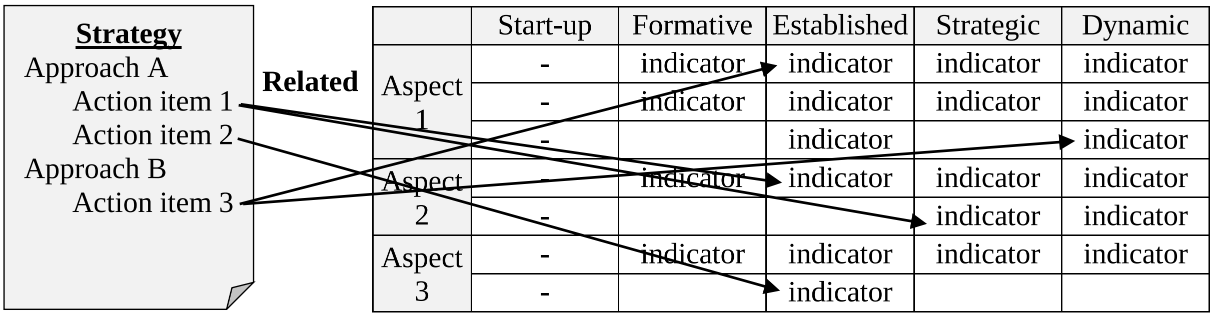

Figure 6. “Mapping”

Result of Comparison and Findings

Result of Comparison

The result of comparison is shown in the **Table 1**.

Please note that the ‘Start-up’ stage is omitted from the table. The ‘Start-up’ stage is the lowest stage and the nation who doesn’t achieve the ‘Formative’ stage (2nd stage) will be automatically positioned as the ‘Start-up’. The indicators of the ‘Start-up’ are not the kind of criteria, but the explanation of the state. Therefore, there’s no cybersecurity approach to have a relation with the indicators of the ‘Start-up’.

The red coloured cells indicate the achieved stages while the blues are unachieved.

Please also note that the official UK assessment was done with the CSCMM (v1.2) and my comparison work is based on the CSCMMN (Revised Edition). The newer version has 24 factors while the older has 20 (4 factors combined into 2, and 6 factors added). The white cells mean the factors are not officially assessed.

Table 1. Result of Comparison (aggregated by Factor)

#	Dimension	Factor	2nd	3rd	4th	5th	T
11	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	0	0	1	6	7
12		Incident Response	0	3	10	6	19
13		Critical Infrastructure (CI) Protection	0	1	7	5	13
14		Crisis Management	0	2	4	5	11
15		Cyber Defence	0	1	14	16	31
16		Communications Redundancy	0	0	4	3	7
21	Cyber Culture and Society	Cybersecurity Mind-set	0	0	2	4	6
22		Trust and Confidence on the Internet	0	4	2	5	11
23		User Understanding of Personal Information Protection Online	0	0	0	0	0
24		Reporting Mechanisms	0	2	0	0	2
25		Media and Social Media	0	0	0	0	0
31	Cybersecurity Education, Training and Skills	Awareness Raising	0	1	7	6	14
32		Framework for Education	0	9	16	31	56
33		Framework for Professional Training	0	2	11	6	19
41	Legal and Regulatory Frameworks	Legal Framework	0	0	1	14	15
42		Criminal Justice System	0	0	10	7	17
43		Formal and Informal Cooperation Frameworks to Combat Cybercrime	0	1	5	5	11
51	Standards, Organisations, and Technologies	Adherence to Standards	0	10	9	0	19
52		Internet Infrastructure Resilience	0	1	4	0	5
53		Software Quality	0	2	1	0	3
54		Technical Security Controls	0	5	3	13	21
55		Cryptographic Controls	0	0	0	4	4
56		Cybersecurity Marketplace	0	0	5	11	16
57		Responsible Disclosure	0	0	0	0	0
D1	Cybersecurity Policy and Strategy		0	7	40	41	88
D2	Cyber Culture and Society		0	6	4	9	19
D3	Cybersecurity Education, Training and Skills		0	12	34	43	89
D4	Legal and Regulatory Frameworks		0	1	16	26	43
D5	Standards, Organisations, and Technologies		0	18	22	28	68
Total			0	44	116	147	307

🟥 achieved 'Stage' 🟦 unachieved 'Stage' □ 'Factor' doesn't exist in v1.2

Findings

The factors 'User Understanding of Personal Information Protection Online', 'Reporting Mechanisms', 'Media and Social Media' and 'Responsible Disclosure' have no or few relations. It means the UK is not eager to develop their capacities in these fields.

The UK's current standings in both 'User Understanding of Personal Information Protection Online' and 'Responsible Disclosure' are 'Established' stage (3rd stage). The UK may possibly be satisfied with the current achievement, although I suspect not.

The factors 'Reporting Mechanisms' and 'Media and Social Media' are the newly added factors in the CSCMMN. The UK may have been unenlightened to those fields when they formulated the strategy.

Otherwise, there's no factor where the comparison reveals the UK cybersecurity approaches are insufficient nor inappropriate – most of the relations are concentrated to the blue zone, i.e. the stages to which the UK is supposed to aim at stepping up while the reasonable portion of the relations are allocated to the highest stages of the red zone, i.e. the stages which the UK is supposed to aim at maintaining.

Conclusion and Research Plan

According to our analysis, the UK cybersecurity strategy looks almost sufficient and appropriate with some areas which include few approaches to enhance capacities and, therefore, may need further examination whether the nation already has adequate capacities in these areas.
This result means;

- Carefully formulated cybersecurity strategies still need review.
- The method to "map" the approaches to the CSCMMN should work.

But it is not clear yet that the CSCMMN is the best tool to which the approaches are "mapped". There may be better tools for that purpose, or we think we could create one.

My future research will include;

- Review other nations' cybersecurity strategies to prove necessity of the strategy review,
- Seek for improvement of the method and
- Search for the better analysis tools.

References

Global Cyber Security Capacity Centre "Cyber Security Capability Maturity Model (CMM) –V1.2" <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf> (Referred on 5 May 2018)

Global Cyber Security Capacity Centre "Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition" <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf> (Referred on 5 May 2018)

Global Cyber Security Capacity Centre "Cybersecurity Capacity Review of the United Kingdom" <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf> (Referred on 5 May 2018)

Global Cyber Security Capacity Centre "Cybersecurity Capacity Review of the Republic of Uganda" <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Uganda%20CMM.pdf> (Referred on 5 May 2018)

Global Cyber Security Capacity Centre "Cybersecurity Capacity Review of the Republic of Senegal" <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Senegal-Report-v4%20.pdf> (Referred on 5 May 2018)

Global Cyber Security Capacity Centre "Building Cyber-security Capacity in the Kingdom of Bhutan" <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Bhutan_September_2015.pdf> (Referred on 5 May 2018)

Global Cyber Security Capacity Centre "Cybersecurity Capacity Assessment of the Republic of Kosovo" <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Kosovo_June_2015.pdf> (Referred on 5 May 2018)

Government of UK "The UK Cyber Security Strategy" <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> (Referred on 5 May 2018)

Government of UK "National Cyber Security Strategy 2016-2021" <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> (Referred on 5 May 2018)

ITU (International Telecommunication Union) "Global Cybersecurity Index (GCI) 2017" <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf> (Referred on 5 May 2018)

The New York Times article on 30 Apr. 2016 "Hackers' $81 Million Sneak Attack on World Banking" <https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html> (Referred on 5 May 2018)

Oath Inc. news release on 3 Oct. 2017 “Yahoo provides notice to additional users affected by previously disclosed 2013 data theft” <https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/> (Referred on 5 May 2018)

SANS ICS Defense Use Case March 18, 2016 “Analysis of the Cyber Attack on the Ukrainian Power Grid” <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf> (Referred on 5 May 2018)

SANS ICS Defense Use Case No.6 August 2, 2017 “Modular ICS Malware” <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf> (Referred on 5 May 2018)

Tagawa Y. and Hayashi K., “Information Sharing and the Core Institution for Cybersecurity”, Bulletin of Institute of Information Security, Vol. 9, PP. 17-44, 2017 (Japanese only)

The United States Executive Order 13687 of January 2, 2015 “Imposing Additional Sanctions with Respect to North Korea” <https://www.federalregister.gov/documents/2015/01/06/2015-00058/imposing-additional-sanctions-with-respect-to-north-korea> (Referred on 5 May 2018)