DPRK's Offensive Cyber Capability

- tactics/technology change in 2012-2013 -

Koichiro Komiyama (komiyama@keio.jp)
Doctoral Student, Graduate School of Media and Governance, Keio University

June 2018

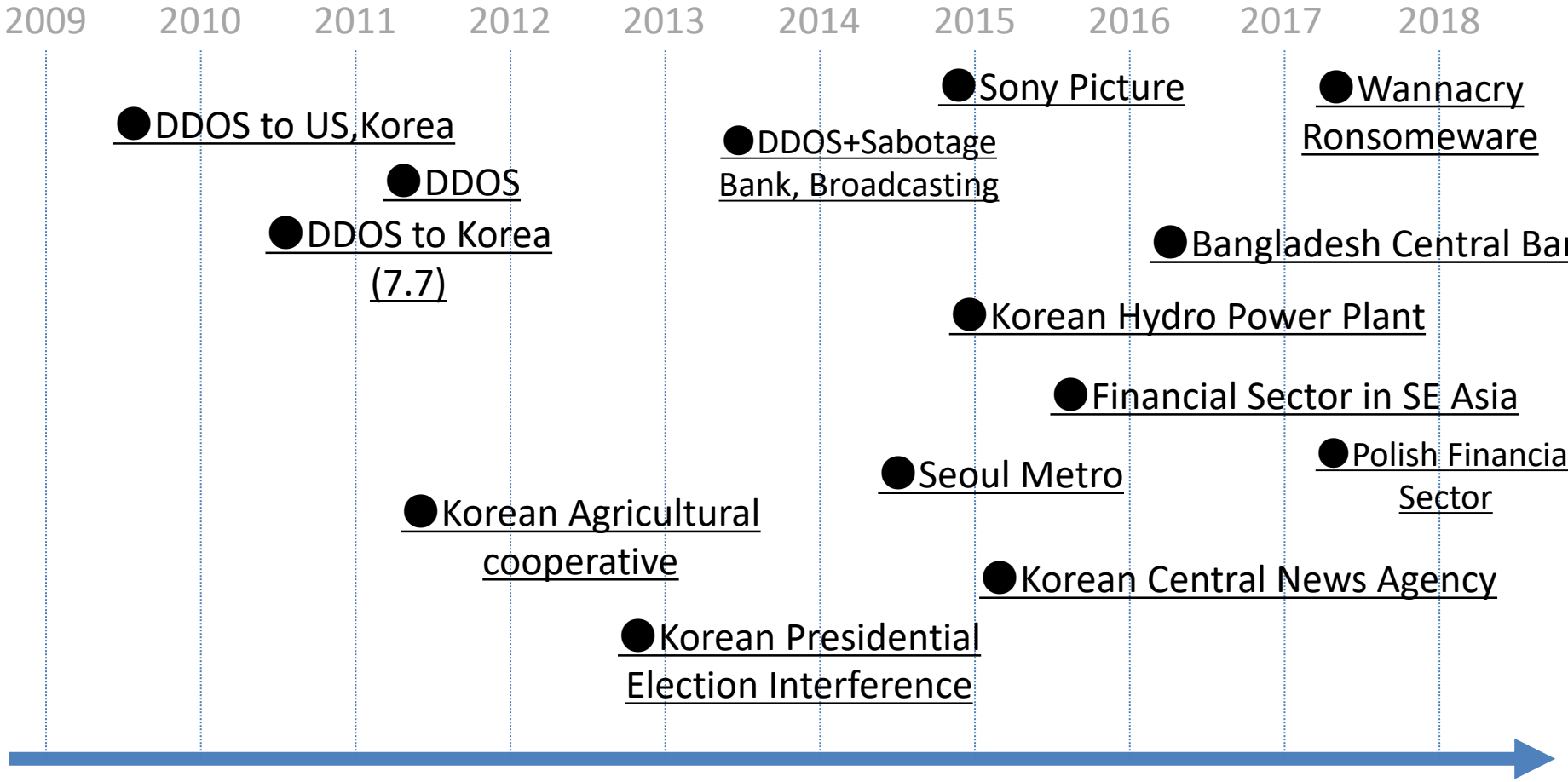
RQ and Analytic Framework

- To measure DPRK's offensive cyber capability, capacity. Especially on how Techniques-Tactics -Procedures has been changed?
- Analytic Framework

  Tri-layered Model

  – Incident Layer: observed, detected attack
  – Tech Layer: development, infrastructure
  – Policy/Strategy area: Key strategic decision(s)

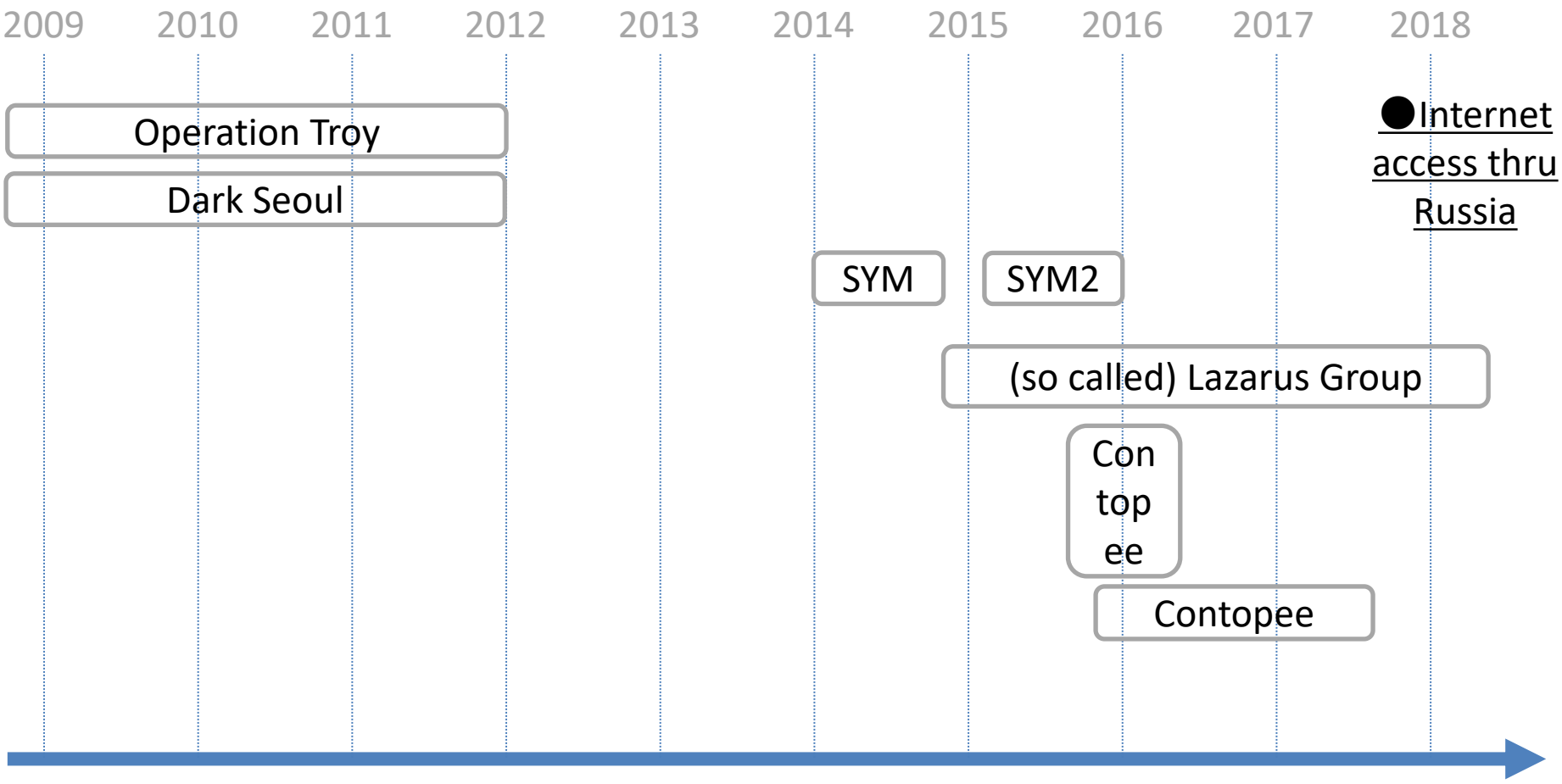
DPRK activity on Incident Layer



Key Findings

- Offensive cyber capability development is consistent since from 2009.
- shift in the motivation of attacks.
  - Financially motivated attack are seen only after late 2014.
  - From sabotage to espionage.

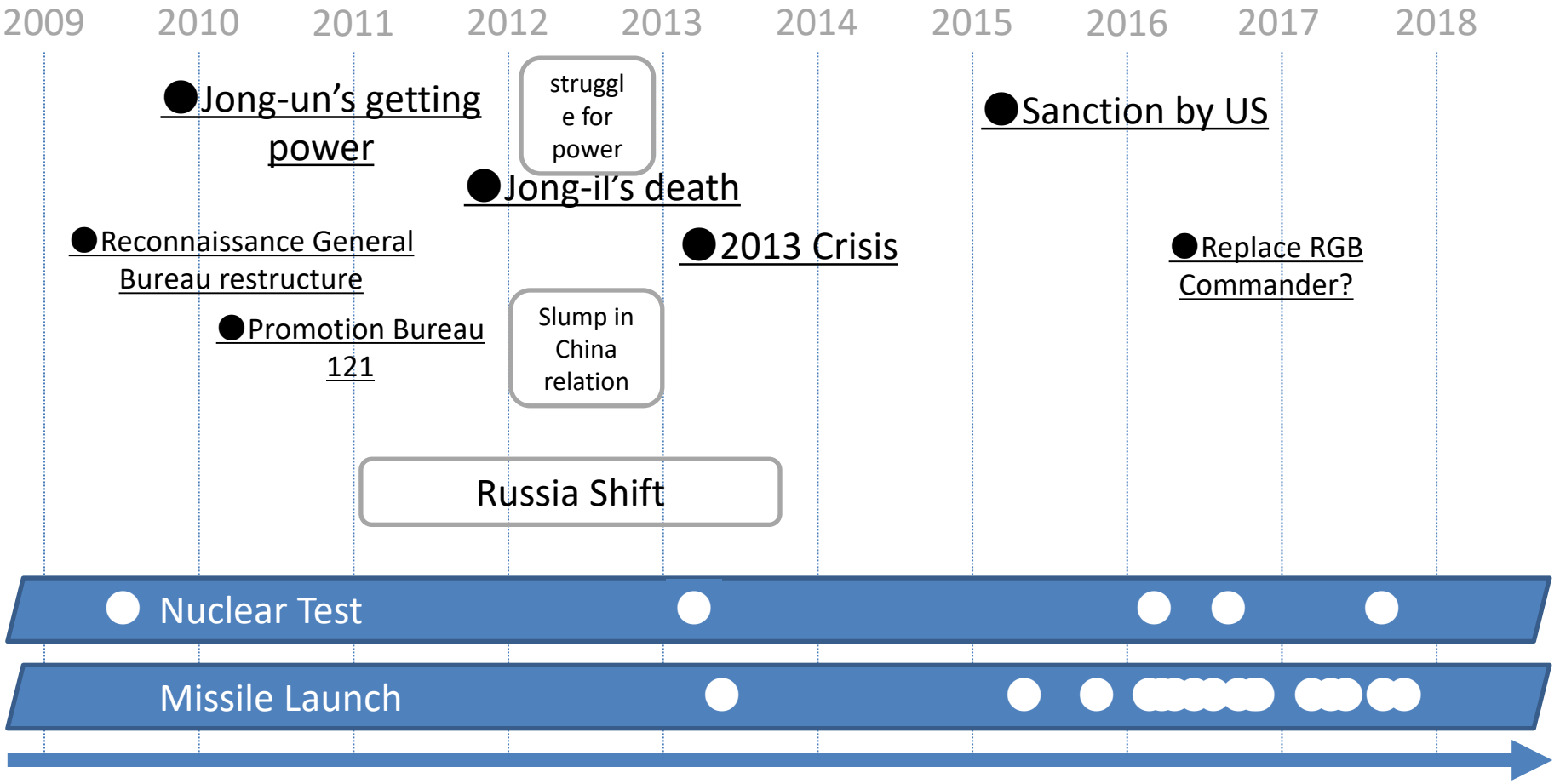
on Tech Layer



Key Findings

- Offensive capability could date back to 2009.
- Very few activities/capabilities from early 2012 to end of 2014.
- China has lost their critical influence over DPRK Cyber activities.

on Policy/Strategy layer



Key Findings

- Power vacuum in around 2012
- Amount of Arms export have been increasing. $30M-50M(2016)

Working Hypothesis need to look further

- Strategy change around 2012-2013 indicates
  A) Undetected, unreported DRPK attack.
  B) Malware development process has changed due to leadership change in military.
  C) Power game after Jong-il's death disturb on the ground operation.
  D) DPRK got new mentor/supporter.

References

Incident

Lewis, J. A. (2009). The “Korean” Cyber Attacks and Their Implications for Cyber Conflict.

対南宣伝扇動で約３００のＳＮＳアカウント運営：東亜日報. (2013, October 29). 東亜日報. ソウル. R

土屋大洋. (2017). 大規模サイバー攻撃は本当に北朝鮮によるものか. 東亜, 601, 6–7.

Tech

Insikt Group. (2017). North Korea’s Ruling Elite Are Not Isolated. Retrieved from https://go.recordedfuture.com/hubfs/north-korea-internet-activity.pdf

Kaspersky Lab’s Global Research & Analysis Team. (2014). The dark story of Darkhotel – Kaspersky Lab official blog. Retrieved September 20, 2017, from https://www.kaspersky.com/blog/the-dark-story-of-darkhotel/15022/

Novetta. (2016). Operation Blockbuster - Unraveling the Long Thread of the Sony Attack, 58. Retrieved from https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Global Research & Analysis Team. (2017). Lazarus Under the Hood. Retrieved from https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf

Shen, A., & Park, M. (2017). A Deep Dive into the Digital Weapons of North Korean Cyber Army. In Hackinthebox (Ed.), hackinthebox. Retrieved from https://gsec.hitb.org/materials/sg2017/D1 - Ashley Shen and Moonbeom Park - A Deep Dive into the Digital Weapons of the North Korean Cyber Army.pdf

Policy Strategy and others

Jun, J., LaFoy, S., & Sohn, E. (2015). North Korea’s Cyber Operations.

Williams, M. (2017). Russia Provides New Internet Connection to North Korea | 38 North: Informed Analysis of North Korea. Retrieved October 2, 2017, from http://www.38north.org/2017/10/mwilliams100117/

Siers, R. (2014). NORTH KOREA : The Cyber Wild Card. Journal of Law & Cyber Warfare, 1, 1–12.

Hearn, K., Williams, P. A. H., & Mahncke, R. J. (n.d.). International Relations and Cyber Attacks: Official and Unofficial Discourse. http://doi.org/10.4225/75/57a82cadaa0e0

Feakin, T. (2013). Playing Blind-Man’s Buff: Estimating North Korea’s Cyber Capabilities. International Journal of Korean Unification Studies, 22(2), 63–90.

Wheeler, D. A., & Larsen, G. N. (2003). Techniques for Cyber Attack Attribution.