Contribution ID: **139** Type: **Paper Abstract (Closed Panels)**

The strategic adoption of Artificial Intelligence by ransomware groups

I examine how ransomware groups –groups of hackers who encrypt stolen data and financially coerce victims to pay to recover the data –adopt Artificial Intelligence (AI) in their operations. I show that many ransomware groups stand to gain a number of operational advantages from AI, including identification of target vulnerabilities, prediction of victim response, and assistance to negotiation and fund extraction. However, most groups have not exploited AI programs because they contain major challenges, including risks of detection and uncertainty of product quality. The article demonstrates that adoption of emerging autonomous technology is a risky business for hacking entities, which is why there is only a small number of instances in which hackers have used AI to extort digital victims for payment. This suggests that ransomware groups rational actors who closely study merits and demerits of AI and that they use reason and risk analysis to make decisions on the selection of technologies they deploy.

What discipline or branch of humanities or social sciences do you identify yourself with?

political science, IR, cybersecurity

If you are submitting an Open Panel proposal, have you included all four abstracts in attachment?

No, I am submitting a Closed Panel abstract

Are you a PhD student or early-career researcher?

No

Primary author: KATAGIRI, Nori (Saint Louis University)

Presenter: KATAGIRI, Nori (Saint Louis University)