

## 10 CYBER SECURITY AND AI

PJD's opening remarks

In the 1960s, research in computer networks and operating systems made it possible for large numbers of users to share access to a common file system. This enabled data sharing and at the same time demanded data protection. Ever since, a major concern of operating system designs has been mechanisms for giving users control over their data and allowing access only with their explicit permission. The ideal default was least privilege – no access or sharing unless explicitly authorized.

This ideal has been devilishly hard to realize. Password systems were not foolproof at keeping intruders out and the network only gave them more ways to try to get in. Among the first attempts to thwart this was intrusion detection systems, which built statistical profiles of actions taken by authorized users and flagged users that deviated from their profiles. Intrusion detection was an early form of machine learning.

Malware, which began as a new threat in the 1980s, became a plague in the 1990s as the Internet connected more and more computers. Malware seeks to steal private data. New kinds of protective machine learning are now part of anti-virus software installed on every operating system.

In the 2000s, search engines began to keep records of every search performed by every user, and then attune ads to the user. This was a way to keep search “free” and still produce revenue for the search companies. Soon thereafter, apps quietly collected data on user action patterns and forwarded the data to app developers. The data are used by machine learning algorithms to predict user responses and preferences and tempt them with hard-to-resist ads. Users have begun to react negatively but no one has found a way to stop the tide of machine learning algorithms users perceive as spies. The old principle of least privilege has been eviscerated by machine learning that can infer your private data from records of your actions.

This concern has given birth to a new research area, cyber security in the age of artificial intelligence. Cryptographers have joined the fray, offering their knowledge of cryptographic protocols as tools that might restore users control over data about their own actions.

Today's speaker is Professor Britta Hale from the computer science department. She will give you a picture of the new security problems and the research that is trying to solve them. She joined NPS a year ago. She holds a Masters degree in Mathematics of Cryptography and Communications from Royal Holloway University of London, and a PhD in the same area from the Norwegian University of Science and Technology. She has been active in protocol design for the Internet Engineering Task Force, which provides standards for the Internet. She has worked in industry research on European nation-level security preparedness.