Strategic Cyberdefense

Dr. Sandro Gaycken

- Director, Digital Society Institute, ESMT Berlin
- Project Director, NATO SPS
- Lecturer, NATO Defense College
- Fellow, Oxford University Martin School
- Advisor, AI Initiative, Harvard Kennedy School
- Founder & Chief Scientists, Hensoldt Cyber Ltd
- Founder & CEO, GOROOT Ltd.

NATO
OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme

Military cyberdefense is a strategic priority

- Military communication, C&C, weapons and platforms are all built on COTS and highly vulnerable
- Hostile hackers of any potential adversary can simply switch off all machinery or manipulate information in critical moments
- Civil targets could be attacked, subversive tactics could cause strategic surprise

NATO
OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Technical IT-security does not solve the problem.

- Technical IT-security is not working properly
- The environment to be protected is too complex and has too many attack vectors
- IT-security paradigms are outdated and dysfunctional
- Detection, Firewalls, Threat Intelligence, AI – all of this only delays attackers, nothing stops them

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Nor does international diplomacy.

- UN GGE has been the most significant effort in this space, trying to define cyber norms
- States couldn‘t agree on anything and want to preserve their industrial and offensive options
- Surveillance and censorship have been difficult issues
- States are now looking at „like-minded“ or bilateral solutions

NATO
OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme

Why is it a multidimensional strategic issue?

- It interferes with every strategy you could possibly have – everything has a cyber component
- It is not just a military issue. The entire government, the industry and civil society must be prepared
- Strategies must address many levels

NATO
OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Why is it a multidimensional strategic issue?

- A military cyberstrategy must address many military and industrial issues
  - Education and training
  - Technical risk management and current vulnerability
  - Educating defense suppliers, building cyberdefense suppliers
  - Legal issues
  - Cyberstrategies and tactics, escalations, cross-domain effects and responses

NATO
OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

We are doing better, but not good.

- NATO community is putting a lot of effort into this, but getting it right is incredibly difficult, even with NATO budgets
- Very high complexity, a lot of smoke and mirrors, politically unattractive topic, no leadership, cautious investors
- Some very good efforts: cyber range, incubator
- NATO community is getting better, but too slow

NATO
OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme

We need to try harder!

- Real cyberdefense still needs to be built from ground up
- Entire technical architectures need to change
- A specialized industry first needs to be built
- Old legacy systems have to be replaced
- Workforce has to be built, too
- A new mindset among militaries is required

NATO
OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme

This workshop is important.

- A majestic strategic challenge lies ahead of us
- Cooperation is key in this difficult situation
- We are, and I am personally, very honored to talk to Japan about this and evaluate common ground and common values
- We are certain to forge a lasting relationship and create real value for all of us

NATO
OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme