UK Cyber Strategy and Future Cyber Threats

GODFREY GASTON

2023
HACKTHEON
SEJONG

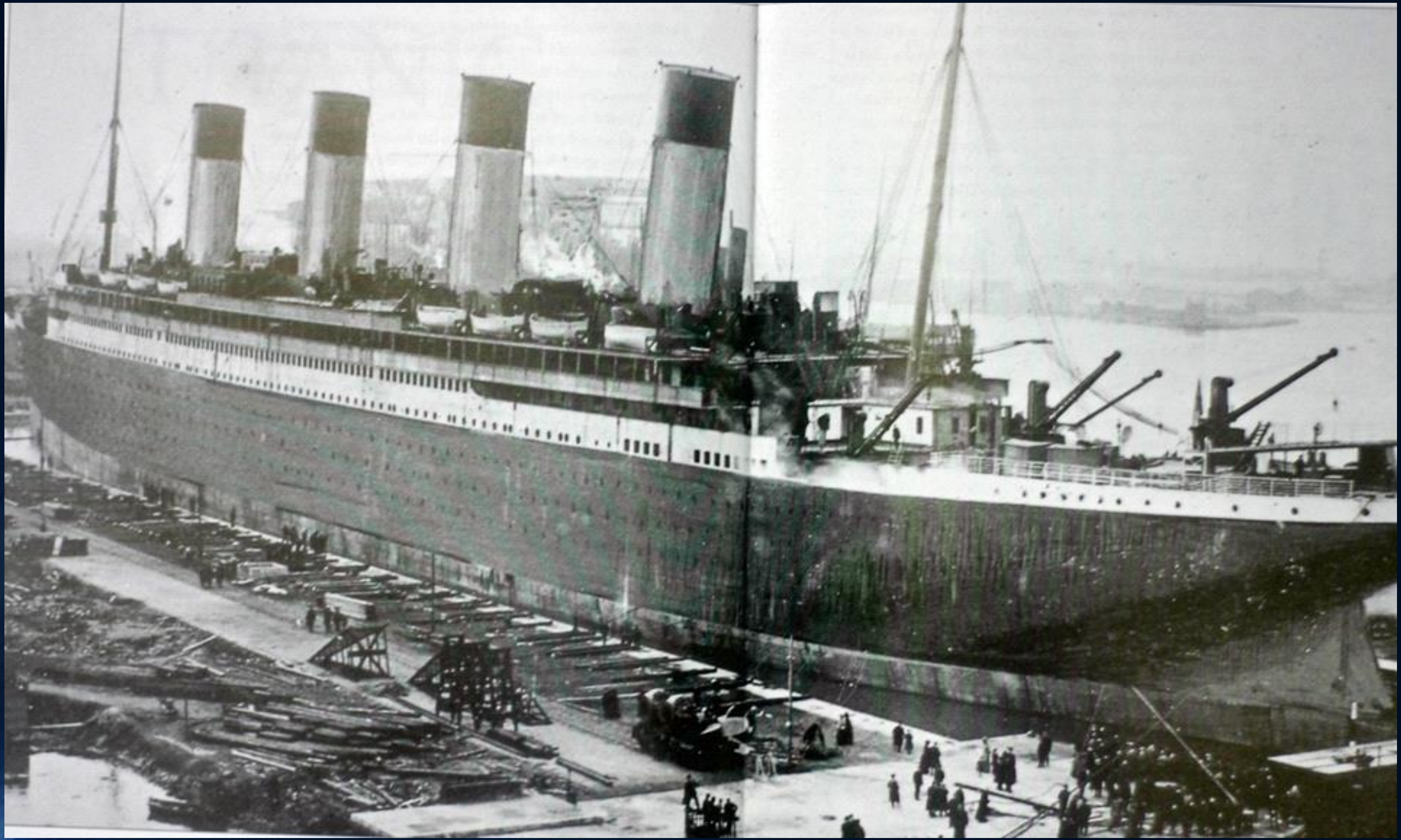
Personal Introduction

- MEng Elect & Electronic Eng – Queen's University Belfast
- PhD University of Edinburgh
- MBA Henley Management College
- Recently retired – Exec Director – Institute of Electronics, Communications and Information Technology – Queen's University Belfast
- Founder of Titan IC technology startup – acquired by NVIDIA March 2020
- Visited Korea about 8 times – Seoul & Daejeon (mostly cyber security collaboration)
- Advisor to swIDch (Korean cyber company in London - SSenstone)

Presentation overview

- Northern Ireland (NI) overview
- Similarities and differences between NI and Korea
- UK National Cyber Strategy
- Future Cyber Threats
- Conclusions

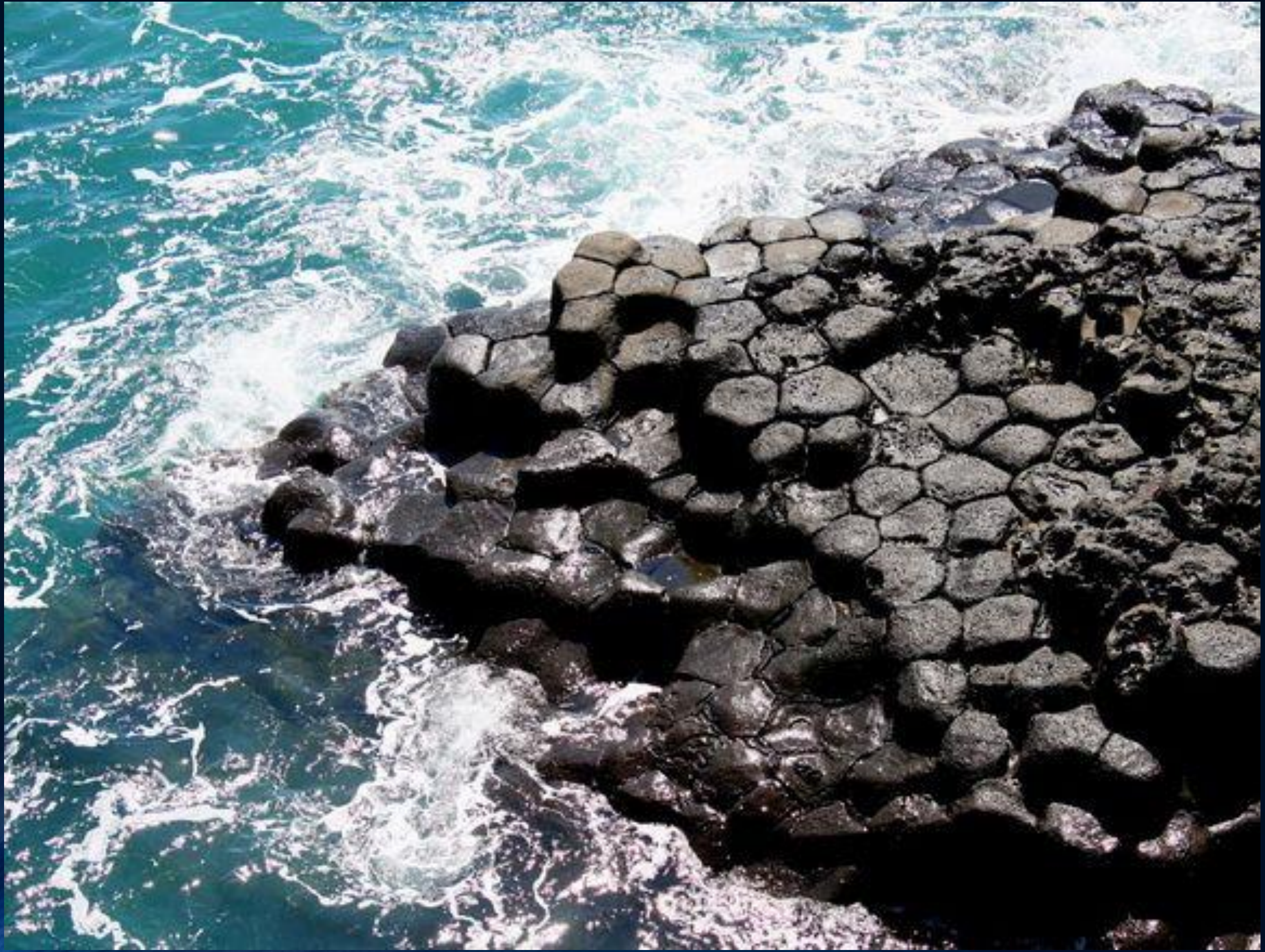
Home of the Titanic



Home of the world's oldest whiskey distillery

Home of the Giant’s Causeway

Just like Jeju Island



Home of great golf courses – Royal Co Down

Home of great golf courses – Royal Portrush

Home of 2 great Universities

- Queen's University Belfast
  - Member of elite Russell Group Universities in the UK
  - Hilary Clinton Chancellor
  - 25,000 students, 3900 staff

- Ulster University
  - 27,000 students, 2700 staff

Similarities between NI and Korea

- Hard working, sense of pride and strong commitment to the task
- Strong family ties, strong emphasis on hospitality and making people feel welcome
- Love to have a party and especially involving alcohol
- Working relationships once established will be long lasting and strong

Differences between NI and Korea

- Strong respect shown for elderly/authority in Korea
- Work environment in NI is less formal and less hierarchical
- Food is completely different – much larger portions in NI also!
- In NI, government is more accountable and questioned more by the voting public
- Language (obviously) but can make for slower progress in business

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SECURING OUR DIGITAL TOMORROW

QUEEN'S UNIVERSITY BELFAST

EST 1845

Research

Securing Connected Systems

Cores areas of expertise:

- Secure Connected Devices
- Networked Security Systems
- Industrial Control Systems (ICS) Security
- Security Intelligence

UK National Cyber Strategy – 2022

Built on 5 main pillars

1. Strengthening the UK Cyber Ecosystem
2. Building a resilient and prosperous digital UK
3. Taking the lead in technologies vital to cyber power
4. Advancing UK global leadership and influence for a more secure, prosperous and open international order
5. Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace

UK National Cyber Strategy – Responsibilities

1. Not just about government (National Cyber Security Centre)
   - Many different departments and organisations involved
2. Private sector a key role to play
   - SME – innovation
   - Corporate – major products that solve major issues
3. Academia – new research and innovation
4. Investors and entrepreneurs
5. Citizens – human factors so important

1. Strengthening the UK Cyber Ecosystem

- What makes a good ecosystem? Ensure regional ecosystems are joined up across the UK. Self-sustaining.

- Address the shortage of cyber skills – importance of the cyber professional
  - National Cyber Force
  - Diversity and focus on school education

- Support the growth of the cyber sector – promoting startups and accelerator programmes and assisting all in international markets
  - Area of development for Korea?

2. Building a resilient and prosperous digital UK

- Government and businesses have a better understanding of cyber risk and support citizens

- Government provide Active Cyber Defence (eg illegal websites) and identify supply chain risks
  - KISA role in Korea?

- Ability to report incidents, respond to and recover quickly from incidents
  - Do we spend too much on trying to stop incidents and not enough on fast recovery?

3. Taking the lead in technologies vital to cyber power

- Co-ordinated approach to R&D – govt / academia / industry
- Identify key technologies where the UK needs own capability e.g. Critical Infrastructure protection
- Ensure minimal cyber risk in the roll out of connected devices and the management of the supply chain
- Ensure active participation by different UK organisations at international standards bodies
  - Korea very strong here

4. Advancing UK global leadership and influence for a more secure, prosperous and open international order

- Work with international partners and organisations to help make the UK more secure

- Help promote a free, open, peaceful and secure cyberspace

- Promote UK cyber capability internationally – both for prosperity and for a more secure cyberspace

5. Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace

- Once detected and analysed – share threat information quickly and to relevant organisations

- Make it more difficult to target the UK and ensure legal agility in place to bring to justice

- Use UK cyber capabilities to assist in other areas of non-cyber serious crime

What are the top cyber threats of the future?

AI for cybersecurity

- Traditionally AI used for anomaly detection in e.g.
  - Insurance fraud detection
  - Financial compliance and regulation
- Now being used in more traditional cybersecurity areas
  - Malware detection
  - Insider threat
  - Cyber crime
- What about the security of AI (not just AI for security)
- Also ethics plays a key part in all of this – multidisciplinary approach

Ransomware keeps coming

- UK’s National Cyber Security Centre reports 3 times ransomware in Q1 2021 compared to all of 2019
- Appears mostly as phishing emails or spear-phishing emails
  - Often very sophisticated in nature
- Most obvious question is – have you appropriate back up in place?
- Particularly worse with home working and for smaller companies
- 8 x less likely to fall victim of phishing email if appropriate education in place

Hyper-connected world

- 5G is the driver for much of the future cyber and data analytics challenges

- Attack surface has increased significantly
  - Internet of Threats
  - Botnet of Things
  - Internet of vulnerable Things

- 18 Billion connected devices in 2022
  - No longer about the “Internet of screens”

Supply chain uncertainty

- How do you know you can trust your suppliers?
  - Hardware – backdoors?
  - Software – open source?
  - Secure by design
- What about 3rd party risk? What about 4th/5th party?
- Risk management framework needed
  - Cyber Essentials for government suppliers
- Within EU – General Data Protection Regulation (GDPR)
  - Data protection and privacy
  - Large fines for data breach

The Covid Challenge to Cyber

- Covid challenged the world to come up with a vaccine for the virus in record time

- Assume we all going to be a victim of cyber breach or cyber crime

- Not enough money is spend on a quick recovery from the attack – too much on prevention

- **Challenge** – instead of recovering from breach in weeks or months – what about seconds or minutes? What is needed to make this happen?

CSIT Spin out – Titan IC

- Start-up from CSIT, Queen's University Belfast (QUB)
- Route to commercialise IP developed within CSIT over the past 10 years in network processing – 100Gb/s network packet inspection for malware
- Seed funded by Queen's University Belfast and through customer revenue/ grants, and also raised Venture Capital (VC) investment (multiple rounds)
- Employees: 28 Staff - 10 HW (Firmware) engineers, 12 SW engineers
- Acquired by Mellanox/NVDA in March 2020

“So what” from a student perspective……

1. You don’t have to spend your career in a “safe” company
   - You will likely need some experience first before doing a startup

2. You are graduating in a key area and the risks of doing a startup are very low
   - Abundance of jobs if startup doesn’t work

3. From my perspective – better to have tried and failed – would always have been asking “what if”

4. Know your strengths – CEO, CTO, Sales,….etc?

5. The training you will gain in doing a startup will be invaluable for your future career whatever that leads to

Final reflections & advice

- Cyber threats and challenges are only beginning – much more to come with 5G
- Governments can write and implement cyber strategies but need the support of private sector, academia and individuals to succeed
- Don’t rule out the opportunity of either being a founder of a start up or joining a startup
    - Great learning experience

Questions?