Encouraging Digital Security Innovation
The Israeli Eco System
National Risk Management & Innovation

REFAEL FRANCO
Deputy Director General
Head of Robustness Division
Israeli CERT Alert

Palo Alto Networks GlobalProtect portal and GlobalProtect Gateway

- PAN-OS 7.1.18 and earlier
- PAN-OS 8.0.11-h1 and earlier
- PAN-OS 8.1.2 and earlier
- Pulse Connect Secure and Pulse Policy Secure
  - Pulse Connect Secure 9.0R1 - 9.0R3.3
  - Pulse Connect Secure 8.3R1 - 8.3R7

Cybernet platform
Recently, a research describing various vulnerabilities in some SSL VPN offerings was presented at Black Hat. Proof of concept code for some of the vulnerabilities was posted on the Internet, and are now actively exploited. CERT-IL published an urgent alert to all users of Palo Alto, Fortinet & Pulse Secure SSL VPNs, urging them to take immediate action.

Due to our national responsibility to protect the Israeli cyberspace, and our shared concern regarding this threat, I would like to invite you to participate in a conference call with other trusted CERTs, to share with you our findings.

Dear Colleagues,

1. Please find attached a zip file which includes "Samoor", ("the scan tool") along with its operating "readme" technical file.

Invite you to participate at a conference call with other trusted CERT's
ISRAEL CYBER JOURNEY

1/1/2018
NATIONAL CYBER DIRECTORATE

- SECURING ISRAEL’S CYBERSPACE
- SECURING ISRAEL’S LEADING POSITION IN CYBERSPACE
Human Capital – Cyber journey
6 Academic Cyber Research Centers:

- ~180 researchers
- ~330 graduate students
Innovation Labs

- Energy – SCADA / ICS
- Fintech security
- Smart transportation
- Medisec
- POC
- AI, 5G

Israel cyber eco system
Government Involvement Formula

\[ \text{Risk} \times \text{Damage} = \text{Government Failure} \]
Robustness

Cyber robustness is aimed to reducing the attack surface and creating a more difficult environment for offensive rivals actions, at the Israeli cyber space.
Government Involvement

- Lack of knowledge
- Major Risk
- Market Failure
National SCADA lab
Government Innovation Cyber Tenders

- Pioneering Product
- Lowest Price
Heat Map – Risk & Damage Indicators

<table>
<thead>
<tr>
<th>Cyber Infrastructure Assets</th>
<th>Information Asset</th>
<th>Top in Sector</th>
<th>Critical to Emergency</th>
<th>Damage to Public Trust</th>
<th>Governance</th>
<th>A necessity for the public without an alternative</th>
<th>Economic Damage</th>
<th>Human Life</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law Firm</td>
<td>Small to medium database</td>
<td>Rated at 30% less important than the sector</td>
<td>Not significant in an emergency</td>
<td>Partial &amp; temporary damage to public trust</td>
<td>Inconvenience to hundreds of people</td>
<td>Millions of $ Indirect damage to the state</td>
<td>None</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>First Responders</td>
<td>Large private database with the potential to harm civilians</td>
<td>Is rated between 30%-70% of the sector</td>
<td>Emergency products are required</td>
<td>Damage to public confidence that is restored by itself</td>
<td>None</td>
<td>Millions of dollars in direct damage to the state</td>
<td>None</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Large IT Integrator</td>
<td>An information asset of national importance</td>
<td>Ranked among the top 10% in the sector</td>
<td>Participate in national service objectives</td>
<td>Significant damage to the public’s confidence in its rehabilitation took months</td>
<td>An existential difficulty for scores or functional difficulties for thousands</td>
<td>Tens of millions of $ in indirect damage or millions of dollars in direct damage to the state</td>
<td>Several</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Large Food Manufacture</td>
<td>A governmental information asset or a basis for other repositories</td>
<td>Rated part of the 5 most important in sector</td>
<td>Critical emergency service</td>
<td>Serious damage to public confidence in its rehabilitation takes</td>
<td>Undermining the government’s ability to govern</td>
<td>An existential difficulty for hundreds of people without alternatives</td>
<td>Financial damage of millions of dollars or more</td>
<td>Larger than many dozens</td>
<td>4</td>
</tr>
<tr>
<td>Hosting</td>
<td>Very complex data</td>
<td>Ranked among the top 5%-10% of the sector</td>
<td>Essential in an emergency</td>
<td>Emergency products are required</td>
<td>Inconvenience to thousands of people or functional difficulty for hundreds</td>
<td>Tens of millions of dollars in direct damage or millions of dollars in indirect damage to the state</td>
<td>None</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Elections Committee</td>
<td>An information asset of national importance</td>
<td>Ranked among the top 10% in the sector</td>
<td>Participate in national service objectives</td>
<td>Significant damage to the public’s confidence in its rehabilitation took months</td>
<td>An existential difficulty for scores or functional difficulties for thousands</td>
<td>Tens of millions of $ in indirect damage or millions of dollars in direct damage to the state</td>
<td>Several</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Insurance Company</td>
<td>An information asset of national importance</td>
<td>Ranked among the top 10% in the sector</td>
<td>Participate in national service objectives</td>
<td>Significant damage to the public’s confidence in its rehabilitation took months</td>
<td>An existential difficulty for scores or functional difficulties for thousands</td>
<td>Tens of millions of $ in indirect damage or millions of dollars in direct damage to the state</td>
<td>Several</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Bank</td>
<td>An information asset of national importance</td>
<td>Ranked among the top 10% in the sector</td>
<td>Participate in national service objectives</td>
<td>Significant damage to the public’s confidence in its rehabilitation took months</td>
<td>An existential difficulty for scores or functional difficulties for thousands</td>
<td>Tens of millions of $ in indirect damage or millions of dollars in direct damage to the state</td>
<td>Several</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Hospitals</td>
<td>Large private database with the potential to harm civilians</td>
<td>Is rated between 30%-70% of the sector</td>
<td>Emergency products are required</td>
<td>Damage to public confidence that is restored by itself</td>
<td>None</td>
<td>Millions of dollars in direct damage to the state</td>
<td>None</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

IEC – Economy & life Damage (CNI)
Value Chain VS Supply Chain
Supply Chain Eco System

- Supply Chain Methodology
- Global cyber Standards
- Cyber Security Products (lab)
Supply Chain Eco System

- Supply Chain Methodology
- Global cyber Standards
- Cyber Security Products (lab)
Supply Chain Eco System

Supply Chain Methodology

Global cyber Standards

Cyber Security Products (lab)
Innovation Labs

- FC3 – Finance
- Meteor
- SCADA & OT
- Transportation & Aviation
- Biometric & ID
- Cloud & 5G
OECD Global Forum on Digital Security for Prosperity

Session 1 - Strategic Initiatives for Digital Security Innovation

14 November 2019
London

Ioannis Askoxylakis
Cybersecurity Technology & Capacity Building
Digital Society, Trust and Cybersecurity
DG Communications Networks, Content and Technology
European Commission
EU action in cybersecurity

- NIS Directive
- GDPR
- Cybersecurity Act
- 5G
- Contractual PPP
- ISACs
- ENISA
- Certification
- International
- Blueprint
cyber
crisis
- Cybersecurity
EU pilots
- CEF
The Proposal for a European Cybersecurity Industrial, Technology & Research Competence Centre & Network of National Coordination Centres
European Cybersecurity Industrial Technology and Research Competence Centre

Centre's Role:
- Network coordination and support
- Research programming and implementation
- Procurement
- Ensuring synergies between civilian and defence spheres
2021-2027 proposed EU cybersecurity funding sources

Digital Europe Programme
€ 2bn

Horizon Europe
Maximum amount to be specified in line with MFF, strategic planning

Cybersecurity Competence Centre

- Voluntary co-investment (in-kind and financial) by Member States
- Direct Funding
- Voluntary Funding

Capacity building projects
Network of National Coordination Centres
R&D projects
DIGITAL EUROPE - initial funding priorities 1/2

• Support to the network of National Coordination Centres;

• **Key capacity building: the cybersecurity shield**
  Deploying a quantum-secured public communication infrastructure (terrestrial segment) with the aim at deploying Quantum Key Distribution (QKD) in various large-scale networks; Deploying through cyber ranges, with Member States and industry, a European cyber threat information network;
DIGITAL EUROPE - initial funding priorities 2/2

• **Certification scheme(s)**
  Support certification capacities
  Support SMEs to certify their products
  Provide certification testbed;

• **Widening the deployment of cybersecurity tools**
  Support for faster validation and market take-up of innovative cyber security solutions by businesses and public buyers;

• **Supporting the NIS Directive implementation**
  Strengthening the activities started under the current CEF Telecom programme (national authorities, CSIRTs, OES, DSP, …)
HORIZON EUROPE - initial funding priorities 1/2

• Automated security quantification and certification
  Verifiable security, privacy, and ethics

• Resilient infrastructures and interconnected systems
  Advanced cryptography; quantum
  Automated threat prediction, detection and response
  Human factors – risk and crisis management
  Authentication of IoT objects
HORIZON EUROPE - initial funding priorities 2/2

- **Securing disruptive technologies**
  - Security ing AI - 5G - IoT – blockchain – distributed computing
  - Big Data privacy

- **Hardware and supply chain security**
  - Cryptography and its implementation
  - Secure systems, despite vulnerable components
  - Virtualisation
EU pilots to prepare the European Cybersecurity Competence Network

More than €63.5 million invested in 4 projects

- **CONCORDIA**
  - Partners: 46
  - EU Member States involved: 14
  - Key words:
    - SME & startup ecosystem
    - Ecosystem for education
    - Socio-economic aspects of security
    - Virtual labs and services
    - Threat Intelligence for Europe
    - DDoS Clearing House for Europe
    - AI for cybersecurity
    - Post-Quantum cryptography

- **Cyber Security for Europe**
  - Partners: 43
  - EU Member States involved: 20
  - Key words:
    - Cybersecurity for citizens
    - Application cases
    - Research Governance
    - Cyber Range
    - Cybersecurity certification
    - Training in security

- **ECHO**
  - Partners: 30
  - EU Member States involved: 15
  - Key words:
    - Network of Cybersecurity centres
    - Cyber Range
    - Cybersecurity demonstration cases
    - Cyber-skills Framework
    - Cybersecurity certification
    - Cybersecurity early warning

- **SPARTA**
  - Partners: 44
  - EU Member States involved: 14
  - Key words:
    - Research Governance
    - Cybersecurity skills
    - Cybersecurity certification
    - Community engagement
    - International cooperation
    - Strategic Autonomy

More than 160 partners from 26 EU Member States

Current EU funding opportunities
Forthcoming topics in H2020 1/2

- **SU-ICT-02-2020**: Building blocks for resilience in evolving ICT systems. (RIA, 47.00 MEUR 19/11/2019)
- **SU-DS02-2020**: Intelligent security and privacy management. (RIA/IA, 38.00 MEUR 27/08/2020)
Forthcoming topics in H2020 2/2

- **SU-INFRA01-2018-2019-2020**: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe. (IA, 20.70 MEUR 27/08/2020)
- **SU-AI-2020**: Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe (IA, CSA 20.00 MEUR 27/08/2020)
The EU Cybersecurity Act
What's new with the new proposal?

- Focused Mandate
- Adequate Resources
- Permanent Status

enisa
European Network and Information Security Agency
Cybersecurity Certification

A voluntary European cybersecurity certification framework.

...to enable the creation of tailored EU cybersecurity certification schemes for ICT products and services.

...that are valid across the EU
Thank you for your attention!
Opportunities and Challenges to Enable Digital Security Innovation: MIT’s systematic approach to innovation through ecosystems and stakeholders

Dr Phil Budden
MIT School of Management

Here East, London: 14 November 2019
In the new global innovation economy, the world is NOT flat.....

...a growing number of innovation ecosystems with unique comparative advantage that can support such entrepreneurship across sectors...

...and this seems true of cyber/digital security too.
MIT’s approach to Innovation Ecosystems
MIT’s iEcosystem approach recognizes engagement with multiple Stakeholders (not just those in the ‘triple helix’).
In MIT’s Innovation Ecosystem model, we outline this ‘System’
Each Capacity has 5 input categories, combining for ‘innovation-driven entrepreneurship’

https://innovation.mit.edu/assets/Assessing-iEcosystems-V2-Final.pdf
Leaders only then choose a **Strategy** for change (eg to enhance digital security innovation)

By implementing **Strategic Interventions**

- Accelerators
- Hackathons
- Prizes & Competitions
- Early-stage Capital Programs

Designing programmatic/policy interventions (PPIs) based on a region’s **comparative advantage(s)**
The seminar opened with a presentation by Prof. Fiona Murray (MIT) and Dr. Phil Budden (MIT) on MIT’s five stakeholder model for Innovation Ecosystems. The presentation underlined that innovation-driven activity today is highly concentrated in key global locations. Research shows that, within highly concentrated geographic regions, innovation-driven activity is also characterised by significant agglomeration and exchange of resources, strongly grounded in teams building high growth innovation-driven enterprises. These so-called ‘innovation ecosystems’ are multi-stakeholder in nature, with critical roles for government, private corporations, risk capital providers, entrepreneurs, and universities.

2. MIT’s Five Stakeholder Model for Innovation Ecosystems

Figure 1: MIT’s Five Stakeholder Model for Innovation Ecosystems

Given the multi-stakeholder and cross-sectoral nature of cybersecurity, innovation in this field is likely to thrive in such innovation ecosystems.

The success of cyber innovation ecosystems – as with other innovation ecosystems – depends on the capacity to efficiently transition ideas to impact (often in the form of new successful innovation-driven enterprises who may later partner with large corporations for distribution and service provision) which is enabled through a diverse set of programs and policies implemented.

https://innovation.mit.edu/assets/Enhancing-Cybersecurity-The-Role-of-Innovation-Ecosystems.pdf
Given MIT’s ecosystem approach to innovation, what is it that the different Stakeholders need for cyber/digital innovation?
On to the first Session of the Panel…

pbudden@mit.edu
Encouraging Digital Security Innovation