5. A. Part 2. SYSTEMS, EQUIPMENT AND COMPONENTS

CRYPTOGRAPHIC "INFORMATION SECURITY"

5. A. 2. "Information security" systems, equipment and components, as follows:

A. 2. c. Designed or modified to use or perform "quantum cryptography";
Technical Note
"Quantum cryptography" is also known as Quantum Key Distribution (QKD

QED-C LAW TAC, 28 FEB 2022

Export Controls and Quantum Anomalies

Sam Weiss Evans, Harvard

Program on
SCIENCE, TECHNOLOGY & SOCIETY
HARVARD Kennedy School

Why do we have export controls?

Export controls assume

- Goods and technologies of security concern are known → Definability
- Enemies are known → Targetability
- States can keep listed items from known enemies → Controllability

Export control assumptions about science, security, and the state

Technical Note
A 'cryptographic activation token' is an item designed or modified for any of the following:
1. *Converting, by means of "cryptographic activation", an item not specified by Category 5 – Part 2 into an item specified by 5.A.2.a. or 5.D.2.c.1., and not released by the Cryptography Note (Note 3 in Category 5 – Part 2); or*
2. *Enabling, by means of "cryptographic activation", additional functionality specified by 5.A.2.a. of an item already specified by Category 5 – Part 2.*

5. A. 2. c. Designed or modified to use or perform "quantum cryptography";
Technical Note
"Quantum cryptography" is also known as Quantum Key Distribution (QKD).

5. A. 2. d. Designed or modified to use cryptographic techniques to generate channelising codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following:
1. A bandwidth exceeding 500 MHz; or
2. A "fractional bandwidth" of 20% or more;

5. A. 2. e. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, not specified by 5.A.2.d., including the hopping code for "frequency hopping" systems.

Definable

Goods and technologies of security concern are known

ENTITY	LICENSE REQUIREMENT	LICENSE REVIEW POLICY
Huawei Technologies Bahrain, Building 647 2811 Road 2811, Block 428, Muharraq, Bahrain.	For all items subject to the EAR, see §§ 734.9(e)[1], and 744.11 of the EAR, EXCEPT[2] for technology subject to the EAR that is designated as EAR99, or controlled on the Commerce Control List for anti-terrorism reasons only, when released to members of a "standards organization" (see §772.1) for the purpose of contributing to the revision or development of a "standard" (see §772.1).	Presumption of denial.
Marzoghi Ltd., 12-20 Albaba Building 119 Road 1507, Manama, Bahrain.	For all items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.
Mohammed Marzoghi, 12-20 Albaba Building 119 Road 1507, Manama, Bahrain. (See also addresses in the United Arab Emirates).	For all items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.

Targetable

Enemies are known

Controllable

States can keep listed items from known enemies

Proposal process

- Identification of need to control (e.g. ETTAC)
- Determination of non-control (proposal development, ~1-6 months)
- Negotiation of control text (1-3 years)
- Implementation of control text (0-1 year)

From identification of need for list change to implementation normally ~1.5-2 years for US

Proposal process: quantum cryptography (2005)

- Identification of need to control: Brits
- Determination of non-control: 5.A.2.a “Information Security”
- Negotiation of control text: information hazards in Technical working group at Wassenaar
  - Early controls tend to be broad, but also easier to get
- Decontrol notes helped industry:

Limitations of export controls

- **Control dilemma:** by the time security concerns are known, knowledge/tech too widespread for control to be useful

- **Dual-use as a concept:** focuses on downstream applications, instead of the idea that many security issues will come from unknown and unintended consequences of research done with best intentions

Unhelpful and helpful Security assumptions

UNHELPFUL		HELPFUL
We must maintain US leadership in quantum tech	→	Govern as if the US were not the leader in quantum tech
Security governance should be limited to proprietary research (NSDD-189)	→	Security, like ethics, is an inseperable part of any quantum research and innovation process
We know what security means	→	The **process** of deciding security concerns should be a subject of debate

How new assumptions change Strategies for protecting the quantum economy

New Assumption		Governance strategies
Govern as if the US were not the leader in quantum tech	→	International collaboration on governance is essential from lab bench to head of state
Security, like ethics, is an inseperable part of any quantum research and innovation process	→	Train scientists/engineers not to “do good” but to “know whom to call, and when”
The **process** of deciding security concerns should be a subject of debate	→	Understand the limitations of “quantum information” metaphor and how that shapes ability to see security concerns

Beyond export controls: experimentation in security governance

Systematically open and critical of assumptions about science, state, and security within governance

Routinized analysis of limitations of current governance

Data and metrics to assess effectiveness of governance experiments

Enhance data sharing on lessons learned from governance experiments

Sam Weiss Evans

Harvard Kennedy School
79 JFK St
Cambridge, MA 02138

@SAWEvans

samuel_evans@harvard.edu