QIS project

- Joint work with Simson Garfinkel
- Forthcoming as **Law and Policy for the Quantum Age** (Cambridge U Press 2020)
- I am not a physicist
- Quantum Information Science (QIS)
  - Quantum technologies (QT)
    - Metrology & sensing
    - Communications
    - Computing
- What policy choices?
QT: why now?

- China & EU investment explicitly to leapfrog over U.S.
  - Major scientific advances at TU-Delft (Microsoft)
  - U.S. response: $1.2bn authorized
  - Limit is talent
- Electronic warfare / MASINT
- Tech fundamentals easier: commercial products can produce quantum effects
- Some quantum effects do not require supercooling
Quantum effects

- Merger of quantum mechanics and information theory
- At quantum scales, nature is probabilistic and objects have attributes of both waves and particles
  - Nitrogen atoms used for sensing have a diameter of 1.12 Å—alternatively a radius of 56 picometers (pm), 0.056 nanometers (nm) or $5.6 \times 10^{-11}$ meters.
Waves and Particles

These colors are created by interference between two wave fronts: the light reflecting off the front side and the back side of the soap film.

Yet, the Sun's ultra-violet light can dislodge electrons from the surface of metal, producing a slight voltage, while light from the red end of the spectrum can't.
Uncertainty

$\uparrow \leftrightarrow 0^\circ + 90^\circ = \text{all light blocked}$

$\uparrow \swarrow \leftrightarrow \text{Notice the blackest block is } 0^\circ + 90^\circ; \text{ introducing } 45^\circ = 12\% \text{ transmission!}$
Three quantum effects underly QT

- **Superposition**
  - Particles can be in an indeterminate state—0 or 1 or between

- **Entanglement**
  - When particles are entangled, measurement of one causes the other to act in a predictable fashion, even when separated by great distances

- **No cloning**
  - At quantum scales, “observation” is a physical act that influences the quantum state
Quantum sensing

- Most mature QT
  - Atomic clocks, MRI, NMR measure quantum effects
  - Most commonly rely on quantum entanglement and superposition
- Some do not require supercooling
- Nitrogen vacancy chambers as a promising medium
  - These are imperfections in diamonds, places where a single nitrogen atom is trapped by the strong bonds of neighboring carbon atoms
  - The nitrogen atom can be manipulated to produce quantum effects, even at room temp
  - Shining a laser at the nitrogen atom causes it to emit light that reveals subtle variations in the Earth’s magnetic field.
Sensing implications

- Electronic warfare driven
- Quantum radar
- Ghost imaging, see through smoke, around corners
- SIGINT to MASINT
- Interferometry

Charting a New Course: Celestial Navigation Returns to USNA

Story Number: NNS15015-27    Release Date: 10/15/2015 3:34:00 PM

By Lt. j.g. Devin Arneson, U.S. Naval Academy Public Affairs

ANNAPOLIS, Md. (NNS) -- Picture this: A naval vessel is navigating the high seas thousands of nautical miles from land. Suddenly all navigation systems become inoperable. What happens next? What does this mean?
Quantum sonar

- Wu et al (2016) use a magnetic gradient tensor device, a SQUID—superconducting quantum interference device, suspended from a helicopter
- 2000 measurements/second. 1 microsecond time sync between devices in matrix
- If you know the strength and direction of a magnetic field with great precision, what can you find?
  - Mineral deposits, tunnels (including activity in them), infrastructure, hidden matériel
- What does this mean for submarine stealth?
Quantum communication

- Quantum-enhanced classical encryption
  - Quantum key distribution (QKD), because of no cloning, you can tell if your key has been intercepted
  - Quantum random number generation (QRNG), because of quantum randomness, you get enough security to defend against quantum computer cryptanalysis
  - Communication can proceed over standard channels typically with AES

- Quantum communications
  - Uses quantum effects — such as the spin of particles — to communicate information
  - Because of no cloning, one will know if a listener is present
  - Could change the “place” communications happens because of entanglement (but this is still sci fi)
QKD & China

- Relies on entanglement, no cloning
- Distribute AES keys based on quantum randomness, invulnerable to even quantum computers
- Consequential development: China QKD by satellite = OTP distribution
- Strategy to address “pre-positioned devices”
- QKD has been around since the 1990s, why hasn’t it taken off commercially?
Quantum internet — 2 fascinating ideas

- First, use quantum effects to communicate
- Boyd (University of Rochester) working on photon’s spin/orbital momentum to communicate therefore more than 1 bit per photon

We use a seven-dimensional state space

- Second, notion of “teleportation”
- We would need quantum memory (to overcome no cloning) + entanglement (Wehner et al. Science 2018)
Quantum computing basics

- Qubit \( (2^n \text{ power}) \)
  - Many kinds — superconducting, trapped ion, photonic, quantum dot
- Three types of QC
  - Simulation
  - Annealers (leader is D-Wave)
  - NISQs
- Uses
  - Possible answer to slowdowns in classical
  - Optimization
  - Simulation of complex physical processes
  - ML
  - Discover nature of P, NP
QC Challenges

- QC faces difficult challenges
- Mastery of superposition, entanglement
- Most qubits dedicated to error correction
- Keep an eye on Microsofts "topological qubit" — involves splitting electrons!
- Decoherence measured in microseconds
- Many QCs require supercooling (15 millikelvin)(annealing, superconducting, but not ion traps, photonics)
- Error correction complicated by continuous variables
- Software, control systems, etc
- Current NISQs will not scale to general purpose computers
- Significant minority warns of quantum winter
Keep an eye on D-Wave’s annealer

- Qualified claims: “In half of 150 applications, performance/quality approaching/occasionally better than classical”
- Satellite placement
- Vehicular traffic analysis
- Aircraft gate assignment
- Placement of antennae
- Robot picking in warehouse
- Election modeling
Quantum cryptanalysis

- State of the art in factoring
  - 20-bit number using D-Wave 2000 annealer (using 89 qubits) — this is a surprise because annealers were thought to be more limited in function
  - Next gen will have 5,000 qubits
  - 768 bit number using classical computers
- NAS: RSA collapse not likely in the next decade
  - But the problem is transition period to post-Q crypto
- Google: to factor a strong key in a day, “would take 100 million qubits, even if individual quantum operations failed just once in every 10,000 operations.”
- Realistic uses (not your CC numbers)
<table>
<thead>
<tr>
<th>Cryptosystem</th>
<th>Category</th>
<th>Key Size</th>
<th>Security Parameter</th>
<th>Quantum Algorithm Expected to Defeat Cryptosystem</th>
<th># Logical Qubits Required</th>
<th># Physical Qubits Required(^a)</th>
<th>Time Required to Break System(^b)</th>
<th>Quantum-Resilient Replacement Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-GCM [5]</td>
<td>Symmetric encryption</td>
<td>128</td>
<td>128</td>
<td>Grover’s algorithm</td>
<td>2,953</td>
<td>4.61 × 10^6</td>
<td>2.61 × 10^{12} yrs</td>
<td>Move to NIST-selected PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192</td>
<td>192</td>
<td></td>
<td>4,449</td>
<td>1.68 × 10^7</td>
<td>1.97 × 10^{22} yrs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>256</td>
<td>256</td>
<td></td>
<td>6,681</td>
<td>3.36 × 10^7</td>
<td>2.29 × 10^{32} yrs</td>
<td></td>
</tr>
<tr>
<td>RSA [6]</td>
<td>Asymmetric encryption</td>
<td>1024</td>
<td>80</td>
<td>Shor’s algorithm</td>
<td>2,290</td>
<td>2.56 × 10^6</td>
<td>3.58 hours</td>
<td>Move to NIST-selected PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2048</td>
<td>112</td>
<td></td>
<td>4,338</td>
<td>6.2 × 10^6</td>
<td>28.63 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4096</td>
<td>128</td>
<td></td>
<td>8,434</td>
<td>1.47 × 10^7</td>
<td>229 hours</td>
<td></td>
</tr>
<tr>
<td>ECC Discrete-log problem(^c) [7, 8]</td>
<td>Asymmetric encryption</td>
<td>256</td>
<td>128</td>
<td>Shor’s algorithm</td>
<td>2,330</td>
<td>3.21 × 10^6</td>
<td>10.5 hours</td>
<td>Move to NIST-selected PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>386</td>
<td>192</td>
<td></td>
<td>3,484</td>
<td>5.01 × 10^6</td>
<td>37.67 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>512</td>
<td>256</td>
<td></td>
<td>4,719</td>
<td>7.81 × 10^6</td>
<td>95 hours</td>
<td></td>
</tr>
<tr>
<td>SHA256 [9]</td>
<td>Bitcoin mining</td>
<td>N/A</td>
<td>72</td>
<td>Grover’s Algorithm</td>
<td>2,403</td>
<td>2.23 × 10^6</td>
<td>1.8 × 10^4 years</td>
<td>Move away from password-based authentication</td>
</tr>
<tr>
<td>PBKDF 2 with 10,000 iteration(^d)</td>
<td>Password hashing</td>
<td>N/A</td>
<td>66</td>
<td>Grover’s algorithm</td>
<td>2,403</td>
<td>2.23 × 10^6</td>
<td>2.3 × 10^7 years</td>
<td>Move away from password-based authentication</td>
</tr>
</tbody>
</table>
QT & Policy

- What policy issues with QTs force us to confront?
- What are the strategic consequences of QT?
- What are the indications/warnings that an adversary possesses QT?
- How is the technology likely to diffuse?
- What QT countermeasures will arise?
- How to foster a QIS workforce?
- Industrial policy
- Privacy
## QIS Research

<table>
<thead>
<tr>
<th>Nation</th>
<th>Estimated Number of Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>8006</td>
</tr>
<tr>
<td>US</td>
<td>6071</td>
</tr>
<tr>
<td>European Union + national</td>
<td>5819</td>
</tr>
<tr>
<td>EU alone</td>
<td>2520</td>
</tr>
<tr>
<td>Japan</td>
<td>1491</td>
</tr>
<tr>
<td>Canada</td>
<td>1425</td>
</tr>
<tr>
<td>UK</td>
<td>894</td>
</tr>
<tr>
<td>Germany</td>
<td>785</td>
</tr>
<tr>
<td>Foundations</td>
<td>618</td>
</tr>
<tr>
<td>Australia</td>
<td>598</td>
</tr>
</tbody>
</table>
Going Deeper?

• Pay attention to the dramatic developments in sensing. These are not as hyped yet are strategically consequential and data intensive.
• Find ways to start practicing (remember the talent limit)
  • Academic partners
  • Most basic level: free accounts on D-Wave, IBM
• Post quantum encryption + (AES 256)