Notes on “Cyberspace and Infrastructure” by William D. O’Neil

The history of infrastructure attack

- Wars in the past have frequently included significant *kinetic* infrastructure attacks. e.g.
  - 41% US bombing against Germany (1943-45) in WWII was on “transportation targets, largely rail”; 6% on oil etc.
  - 88% of Iraq’s electric infrastructure was disabled in the 1991 Gulf War
- No *military* cyber attacks on infrastructure are publicly known, but there have been “many attacks by hackers”

Networks

- It’s useful to distinguish two types of networks: Uniform-random, and hub-and-spoke
- Cyber networks tend to be hub-and-spoke
- The electrical network is more like uniform-random
- The 2003 blackout led to important lessons
- Smart electric grids of the future must also be secure
- Similar remarks apply to oil and gas pipelines

It's useful to distinguish two types of networks:

- Uniform-random networks: no hubs, most nodes connect to roughly the same number of other nodes
  - Eliminating a small number of nodes cannot cause a large amount of disruption
- Hub-and-spoke networks (also called power-law or scale-free networks): a small number of *hubs* have many connections
  - *Randomly* eliminating a small number of nodes causes little disruption, but eliminating a small number of *hubs* could cause serious disruption

Cyber networks are hub-and-spoke

- The physical infrastructure of the Internet (i.e. routers and cables) and other communications (e.g. phone) form a hub-and-spoke network
  - Therefore, random outages have limited effect, but an attack targeted at hubs could produce serious effects
  - “thus, protection of major Internet hubs is a cornerstone of ... cyberspace infrastructure defense”
  - Important but isolated sites may need multiple redundant physical communication links

The electrical network contrasts with cyber networks

- Electrical networks are “more like” uniform-random networks
- Electrical networks are susceptible to cascading failures
  - The failure of one link increases the load on alternative routes, which might then also fail, and so on
  - However, for technical reasons, cascading failures are unlikely to cross between different regions of the 4-region North American power grid
- Complete deregulation of the electricity industry appears to be incompatible with ensuring stable and safe supply
  - Deregulation has been the major trend since the 1970s

Lessons from a blackout

- August 2003 blackout affected 50 million people in northeastern US and Canada
- The causes were a combination of technological problems and human error, *not* cyber attack
- However, the subsequent investigation revealed vulnerabilities suggesting that cyber attack could have produced a similar result
  - SCADA (supervisory control and data acquisition) and EMS (energy management systems) are of “particular concern”

The (secure) grid of the future?

- The trend towards a smart grid creates even more potential for security problems
- Hence, security must be taken into account when designing smarter systems

Pipeline networks

- Oil and natural gas pipelines present lower risks than the electric grid, but have “parallel concerns”
- Over 60% of US oil is transported by pipeline, and almost all natural gas
- Oil and gas pipelines also use SCADA

Infrastructure threats

- Use of COTS (commercial off-the-shelf) systems for SCADA/EMS increases vulnerability, compared to bespoke systems
- It's not clear whether compromise of SCADA could lead to long-term, irreparable damage
- Software is the most vulnerable aspect of these systems
  - Even with very careful software engineering, security flaws often remain

Do we believe this?

Policy and organization

- Presidential directives and Congressional legislation have prioritized infrastructure protection since 1998 (Clinton directive 1998; Bush directive 2001, Homeland Security Act 2002, etc)
- Little focus on cyber attacks other than the 2003 National Strategy to Secure Cyberspace, which states the private sector is “best equipped and structured to respond to an evolving cyber threat”

Organizational responsibilities

- DoD depends on non-military infrastructure, but does not have the official responsibility for it
- Five other federal agencies have responsibilities for energy infrastructure

Policy issues

- There is a tension between private enterprise and infrastructure security
- Security can be incentivized via market solutions or regulatory solutions, but relying solely on the market appears problematic
- Rational analysis of terrorist threats suggests they may be less than other dangers (e.g. traffic accidents, drownings)

Policy recommendations

- [summarized as a group activity]