Research in the Computer Science Department, U.S. Naval Postgraduate School: Cyberdeception and Cyberwarfare Strategy

Neil C. Rowe

U.S. Naval Postgraduate School

Monterey, California, USA

ncrowe@nps.edu

http://faculty.nps.edu/ncrowe

Degree programs for the NPS Computer Science Department

The U.S. Naval Postgraduate School (NPS) is the graduate school of the U.S. Naval Academy in Annapolis, Maryland.

- About 2000 students in 100 degree programs: 50% U.S. military, 30% foreign military, 20% civilians.
- M.S. and Ph.D. programs in Computer Science
  - Special interest in information security
  - Special interest in networking
- M.S. and Ph.D. programs in Modeling, Simulation, and Virtual Reality
  - Special interest in virtual training environments
- Ph.D. in Software Engineering
- M.S. in Cyber Systems and Operations: Management of military cyberspace defense and offense
- We also work with the Information Sciences Department (management of digital systems) and the Operations Research Department (applied mathematics for analytics).

Prof. Rowe's research interests

- Digital forensics (discussed in talks March 20 and March 25)
- Machine learning with big data (discussed in talk March 27)
- Defensive cyberdeception (subject of his book, *Introduction to Cyberdeception*, Springer, 2016) (discussed here)
- Cyberwarfare strategy and tactics (discussed here)

Many papers on these subjects are available at http://faculty.nps.edu/ncrowe.

Prof. Rowe's digital forensics interests

- Most of it is empirical digital forensics: Analyzing real data of real computer systems.
- We have a collection of 4000 copies of secondary storage from computers and digital devices around the world.
- Particular interests:
  - Identifying forensically interesting files
  - Extracting useful personal artifacts of users: Email addresses, phone numbers, personal names, IP addresses, GPS data, keyword searches, and so on
  - Inferring social networks from a related set of machines
  - Learning where malware is likely to hide on drives
  - Translating natural-language words in file paths
  - Studying the evolution of different versions of executables
  - Distinguishing users based on their time periods of activity

Prof. Rowe's research interests in machine learning and big data

- Anomalies in military sensor data, particularly for aircraft and ship tracking data
- Learning new cyberattacks from analysis of honeypot data, from computer-system decoys on the Internet
- Tracking of people doing physical-motion tasks for training purposes

Prof. Rowe's research interests in defensive cyberdeception

- Cyberdeception is a useful defensively against cyberattacks:
  - Attackers aren't expecting it.
  - Many deceptions are inexpensive to do.
  - You get better intelligence about new attack methods when you deceive cleverly.
- Good defensive cyberdeception techniques:
  - Deliberate delays
  - False error messages
  - Flooding a user with too much information
  - Offering bait files and data
  - Offering fake network nodes
  - Camouflaging a system

Our theory: 32 “semantic cases” for deception

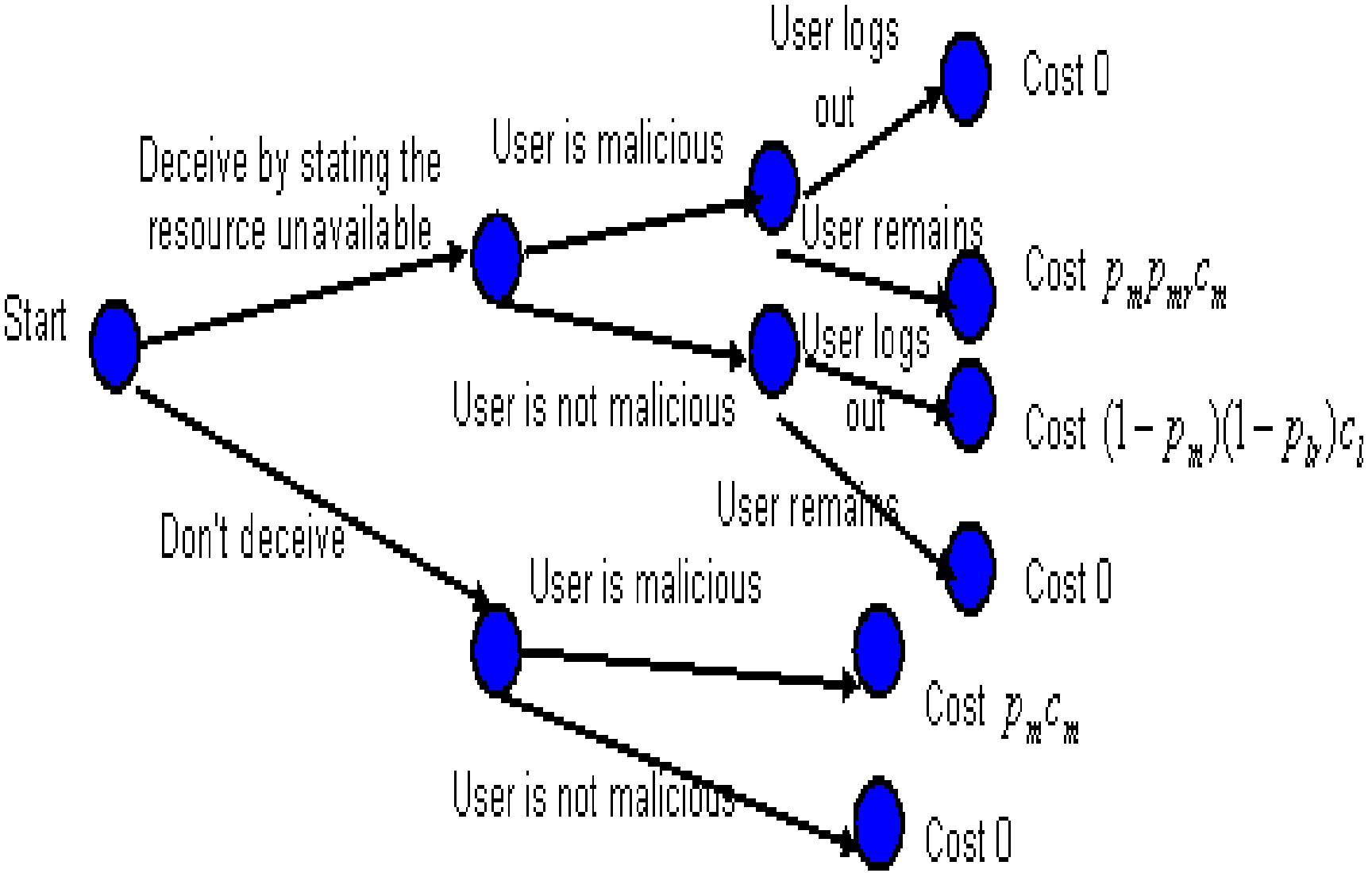
- Space: location-at, location-from, location-to, location-through, direction, orientation
- Time: time-at, time-from, time-to, time-through, frequency
- Participant: agent, object, recipient, instrument, beneficiary, experiencer
- Causality: cause, effect, purpose, contradiction
- Quality: content, value, measure, order, material, manner, accompaniment
- Essence: supertype, whole
- Precondition: external, internal

Some strategies for lying

Suppose you want to do an action X against your enemy.

- **Stealth**: Do X but don't reveal it. Eventually it will be discovered. Common in conventional warfare.
- **Excuse**: Do X and give a false excuse why. Earns respect until excuse found out.
- **Equivocation**: Do X and give a correct but misleading reason why. Like excuse but more coverable.
- **Outright lying**: Do X but claim you didn't. Eventually this will be discovered. Often best method in a crisis.
- **Overplay**: Do X ostentatiously to conceal some other less obvious deception. Exploits the common human tendency to underestimate once one feels superior.
- **Reciprocal**: Give a person a good reason to lie to you so they will pay less attention as you lie to them.

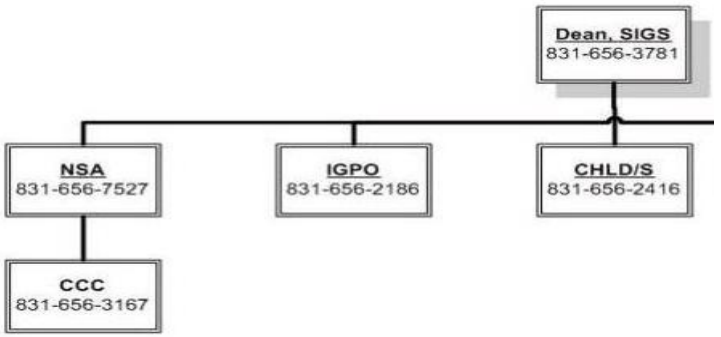
Will our deception hurt us more than them?



A fake directory system

Directory of /root

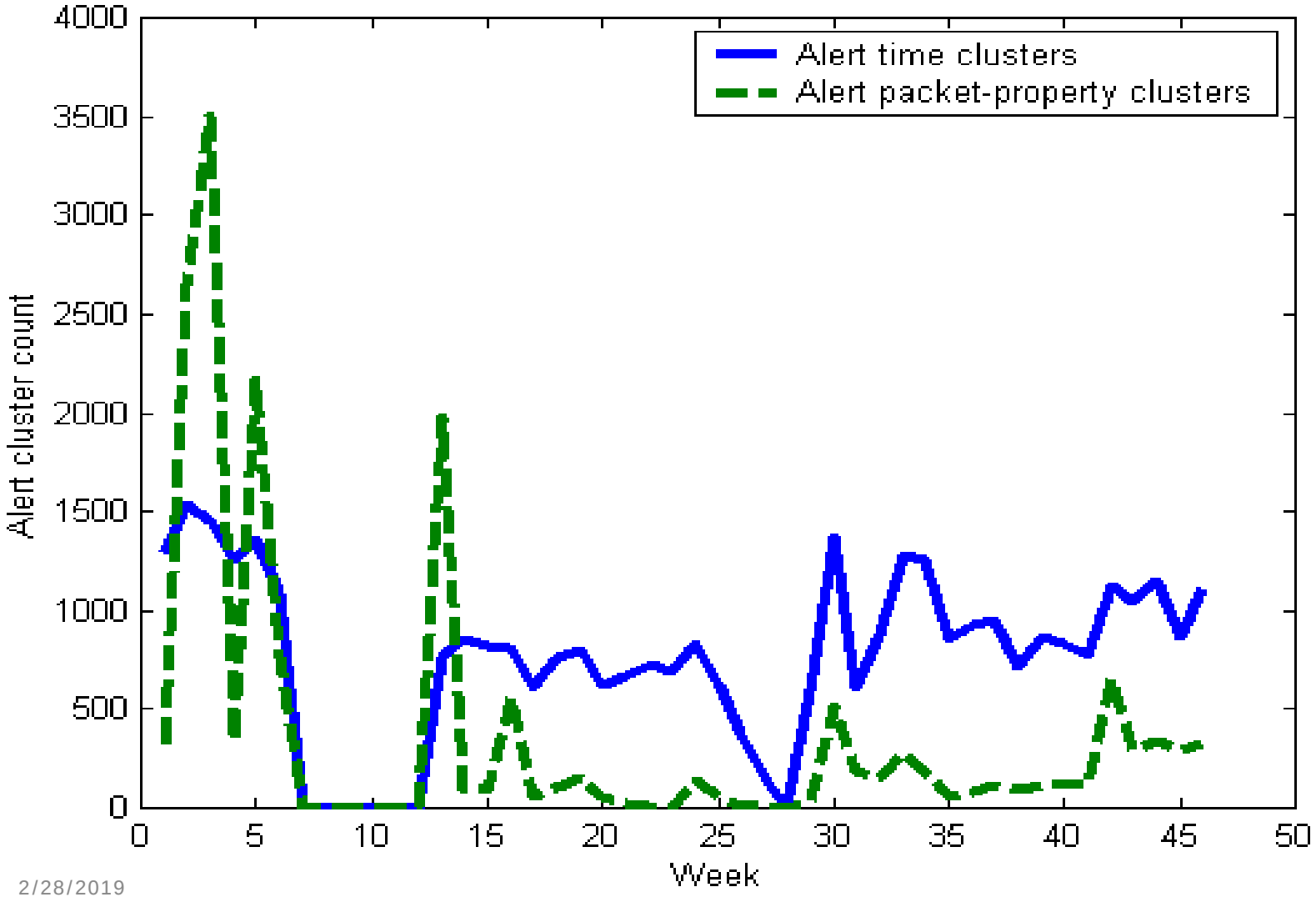
12/24/00 11:44 <DIR> %7Eradlab
12/14/91 21:56 <DIR> PAO
05/02/01 06:14 <DIR> Summer2002
02/23/02 23:39 17 announcement_april_02_2002_picture01.html
09/25/95 03:41 <DIR> dl
05/03/95 23:27 <DIR> ece
11/04/94 10:40 114 events.htm
12/24/98 12:25 <DIR> fsoa
08/02/96 11:49 <DIR> is2020_Net_zg
05/01/96 02:04 <DIR> mosc
03/09/94 22:36 <DIR> oc4213
11/13/96 21:50 89 oldie.htm
07/28/94 04:52 <DIR> or
04/01/96 16:20 <DIR> outdoors
12/26/93 20:49 <DIR> profiler
12/12/01 16:21 24 projecttcx.html
08/16/00 10:22 <DIR> sigs
08/12/00 15:10 104 weather.html
08/27/00 20:46 <DIR> wecs5-tut
05/00/96 20:38 <DIR> ~braccio
04/27/00 17:09 <DIR> ~brutzman



OoqOGc^vLcVuJIDnp}~A}KJWznkQHczA^`snpDGzkoQ~JhGgm
[mNirVBuwnkCNLvVXXyDs|koviWhD`dAsAaOuv[JzOzO
[N~xRzR|xWzH|a□UwIuzEf□[SYz_ngU~vs\AHDoyfHc\nW{}c^FUy]
`tj\zaIYmtTkJaHOtU\\\IAMcPVilyR□ALs~Zd]}
MTqabyzHvEchFroGzeD\OBnOtX|Kaq[u@Vix}
Nzy~db|wHwS□Mt`eZnCS~siyIstkncudzu^CU|FF`zeLI□RH_cjZk}
SQ\ZIVON\{ZQZbRu~sDSXanE[UIa
{kjXws|awo|r□||WwGJFyFUXGJitmuw^HBPDP[o|_oEVBp~iG\tzGX]
OKrv~`_ft`Dy@PKU
[dADqJozwQ_pv@JBNRAujzRTjHJVDP`bj^KJ~jfZLdCSTVh]
OYuoSH|Uki@F[RYeldyNQtc}Kg□LXS|pj}
J|zlaLxZDHp@mszFbKRLcJL^_vD_IQLvM\N□nYP[Yu}GHR
[T|\t\jBjhBuKy}`Q]DgGcEjRdUNtk_LAsbOZJ[Tij^KQkAzVlO
{rbCANtgY|qfG_□hozVZfYBwzZxI}p~K@RLpaZkZSyM]
zgAHG^qo^EXOTBK□□bGt^s\pgScmi\^Br^fR`s|uhg@N`\Rj_nVMVQ
WeJ~qZpV[AoqKAviynigbw@iEEIucpwSK}DNR
[TDYMGPCc|^uJgdKyaq|e`]Xj]u□Gw}
bpdv__zVCRkYNEKyqMgZ\ogc}yPI^kLB~_^fIuqgzgxtGhENs}
□|S□lDXMxGdN_iEntP[UnUsv□OXD
{BO^TRQOTREqVBLB~IyasvvyfXtv]Q}fO
[EXmrEbwXCyUg`GbAEcSmuyRHsX|d[}XA□}\iV~XcshIIGUhqI

Testing of cyberdeception methods on a honeypot

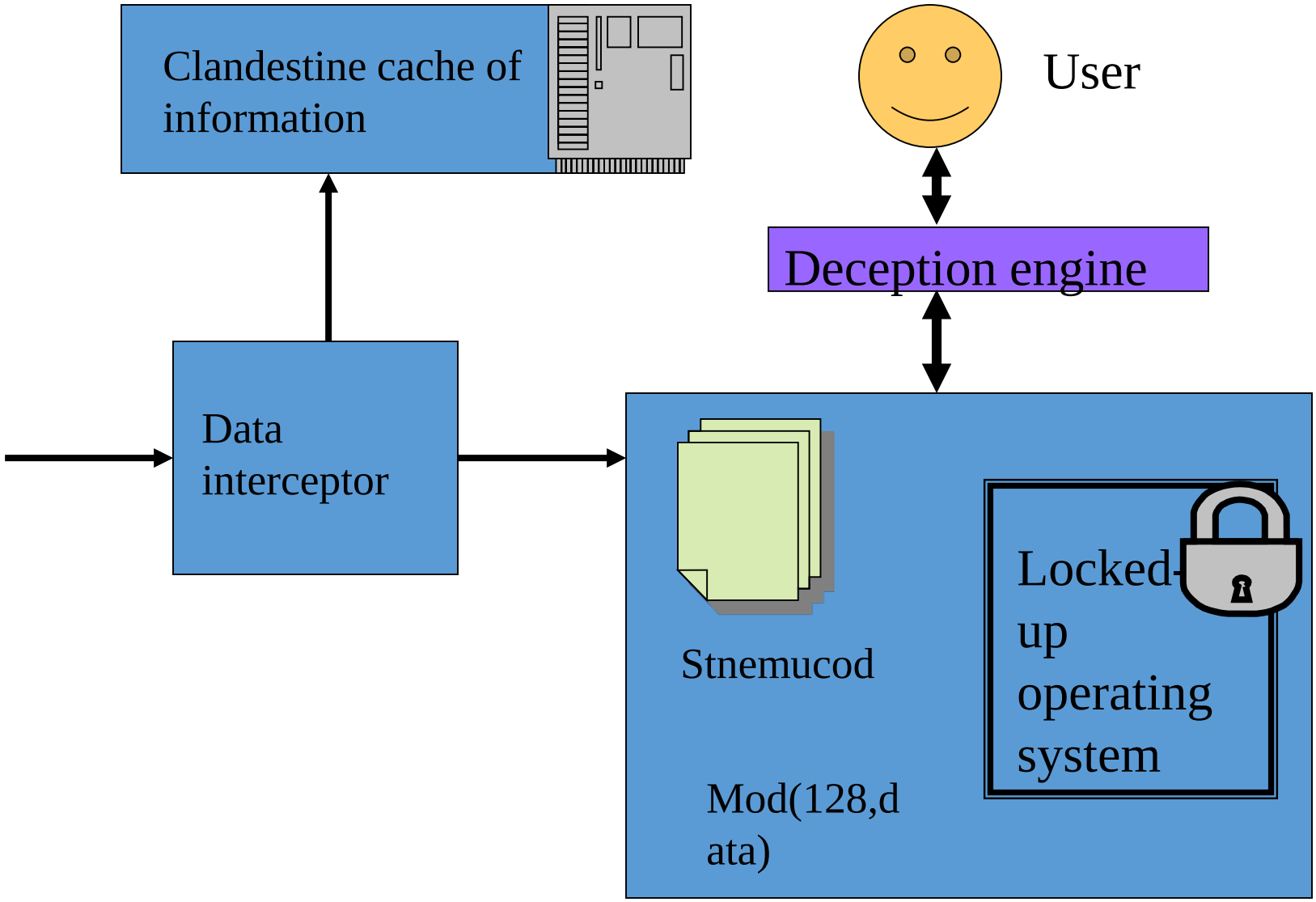
Green shows attack diversity, blue attack volume.



Prof. Rowe's research on cyberwar strategy and tactics

- How can effects of cyberweapons be made reversible? This would make them more ethical to use.
- How do we ensure that cyberattacks distinguish civilian targets carefully?
- How can we attribute cyberattacks to countries or organizations?
- Cyberweapons are usually effective only once. When are good times to use them?
- Cyberweapons aren't very reliable – how many do we need to use together to get a desired success probability?
- Why aren't cyberweapons good deterrents (since our current methods are not discouraging the Chinese and Russians)?

Reversible attacks, visually



How cyberweapons can hit civilians

These are discussed in a YouTube video of my talk at Oxford University.

1. Civilians are easy targets in cyberspace since most of the infrastructure and users are civilians.
2. Dual-use targets are hard to avoid in cyberspace.
3. Civilians can be necessary intermediaries in attacks.
4. Reporting an attack often allows reuse of the attack against civilians.
5. Automatically propagated attacks like viruses and worms don't have sufficient knowledge to recognize civilians.
6. Attackers often spoof civilians, making real civilians more vulnerable to counterattack ("cyber perfidy").

From Addl. Protocol I (1977) to Geneva Conventions

- Article 52 -- General protection of civilian objects

  1. Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph 2.

  2. Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

  3. In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.

Perfidy in the Geneva Conventions Addl. Protocol I

- Article 37 [Link] -- Prohibition of perfidy

  1. It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy. The following acts are examples of perfidy:

  (a) the feigning of an intent to negotiate under a flag of truce or of a surrender;

  (b) the feigning of an incapacitation by wounds or sickness;

  (c) the feigning of civilian, non-combatant status; and

  (d) the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict.

  2. Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation.

The attribution problem

- Attribution of cyberattacks to a country or group is difficult.
- Backtracing requires cooperation of a wide variety of system administrators, something hard to get.
- IPv6 may help – but addresses can still be spoofed.
- Does spoofing violate the warfare prohibition against perfidy?
- Can espionage support backtracing?
- How can we attribute an adversary convincingly for world public opinion?

Norms for cyberwarfare

- Since cyberwarfare is a new domain for which international law will take a while to catch up, we need policy guidelines ("norms").
- We have built a taxonomy of norms.
- Some tough ones:
  - Should we buy exploits since it rewards hacking?
  - Which of our attacks should we acknowledge?
  - What severity of attack is an act of war?
- Cyberweapons are getting serious enough that we should start thinking about cyberarms control.
- Issues to consider:
  - Detection of cyberarms development is possible given that the weapons need much testing against real targets.
  - Detection of cyberarms can be done on captured disks – they look different from regular malware.
  - International agreements can be negotiated.

Table of cyberwarfare norms

What metanorms does a state use for managing other norms?

- Does the state publicise its norms?
- Are norms context-dependent?
- Are norms randomised?
- Do methods permit counterattack? (O)
- Does the state want other countries to use its norms as well?
- Which norms require reciprocity?

What role does cyberconflict play in a national strategy?

- Does the state do cyber operations at all? (O)
- Does it think cyber-operation capabilities deter aggression? (O)
- Is it willing to risk costly counterattacks from cyberconflict? (O)
- Does it allow cyberconflict to entail perfidy? (O)

When and how does a state conduct low-level cyber operations?

- Will the state conduct cyber-espionage?
- Will it conduct cyber coercion? (O)
- What targets will it consider? (T, O)
- How will it reduce the danger of escalation? (T, O)
- How willing is it to share information about vulnerabilities it discovers in cyberspace, both publicly and within its government? (D)
- Can entities other than governments do cyber operations? Will the government police them? (O)

When does a state use cyberattack as an instrument of national policy?

- What level of damage over what time period ensures a state's response? (D)
- How much certainty in the attribution of cyberattacks does it require before it counterattacks? (T, D)
- How does it rate the importance of attack targets? (O)
- Can a non-cyberattack on a state entail a cyberattack response? (O)
- Can a cyberattack on a state entail a non-cyber response? (O)
- To what extent will it attack dual-use (jointly military and civilian) targets? (T, O)
- What counter-cyberattacks of a state will be automated responses? (O, D)

International options with cyberattacks

- International law can mandate reversible attacks, much as it mandates conditions on weapons deployment such as for land mines.
- Possible international responses to cyberattacks:
  - Sanctions and boycotts: Loss of Internet connectivity is a powerful threat.
  - Legal proceedings and fines: Precedents are accumulating.
  - Reparations: Strong international organizations can demand them; required reparations (or required repair itself) are an incentive for reversibility.