Cyberspace and the Changing Nature of Warfare

Kenneth Geers

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Real World vs Cyberspace

• What’s the difference?
• Now integral part of every pol/mil conflict
  – Propaganda, espionage, reconnaissance, even warfare
• The Internet’s amplifying power
  – Victories in cyberspace can become victories on the ground
Cyber Warfare

• Nuclear, Chemical, Biological … Digital?
• Revolution in Military Affairs (RMA)
  – IP-enabled personnel, munitions, sensors, logistics
• Before, during, after fighting
  – I&W, D&D, e-mail campaigns, blog poisoning
• Assassination of computer geeks?
Cyber Warfare Strategy

1. The Internet is vulnerable to attack
2. High return on investment
3. Inadequacy of cyber defenses
4. Plausible deniability
5. Participation of non-state actors
S1 The Internet is Vulnerable

- Imperfect design
  - Hackers can read, delete, modify information on or traveling between computers
- Common Vulnerabilities and Exposures (CVE) database grows daily
  - Difficult to guard all holes into your network
S2 High Return on Investment

• Common attack objectives
  – Research & Development data
  – Sensitive communications
  – Limited only by the imagination

• The elegance of computer hacking
  – Less expensive
  – Less risk

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
S3 Inadequacy of Cyber Defense

- Still an immature discipline
- Traditional skills inadequate
  - New skills highly marketable
- Investigations slowed by international nature of Internet
  - Cultural, linguistic, legal, political barriers
  - No help for state-sponsored operations
Understanding C. Crime

Information Protection Laws

Information Security in Russia

Computer Criminals

C. Crime Units

SORM

Library

Forum

Send an E-mail

http://www.cyberpol.ru/

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Республики:
Отдел "Р" МВД Республики Горный Алтай: Altay
Отдел "К" МВД Республики Мордовия: Mordoviya
МВД Республики Татарстан: Tatarstan
Отдел "К" МВД Республики Чувашия: Chuvashiya
Края:
Отдел "К" УСТМ ГУВД Альтайского края: Altay
Отдел "К" ГУВД Красноярского края: Krasnoyarsk
Отдел "К" УВД Приморского края: Primorskiy
Отдел "К" УВД Ставропольского края: Stavropol'
Области:
Отдел "К" УВД Архангельской области: Arkhangel'sk
Отдел "Р" УВД Владимирской области: Vladimir
УФСБ России по Воронежской области: Voronezh

Отдел "Р" УВД Кировской области: Kirov
Отдел "К" УВД Костромской области: Kostroma
Отдел "К" УВД Липецкой области: Lipetsk
Отдел "К" ГУВД Нижегородской области: Nizhniy
Отдел "Р" УВД Новгородской области: Novgorod
Отдел "К" УВД Оренбургской области: Orenburg
Отдел "К" ГУВД Самарской области: Samara
Отдел "Р" УВД Тамбовской области: Tambov
Отдел "Р" УВД Тульской области: Tula
Отдел "Р" УВД Ульяновской области: Ul'yanovsk
Отдел "К" УВД Читинской области: Chita
Автономные округа:
Отдел "К" УВД Ханты-Мансийского АО: Khanty-Mansi

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Здравствуйте, уважаемый Kenneth Geers!
Можем дать следующие ответы на Ваши вопросы.
Вопрос: Получали ли вы в прошлом запросы об информации из-за рубежа?
Ответ: Да. Каждый день 89 подразделений Национального центрального бюро Интерпола России по E-mail получают и обрабатывают много поручений и запросов от правоохранительных организаций стран - членов Международной организации уголовной полиции Interpol.
Вопрос: Что мешает улучшению международного сотрудничества?
Ответ: Разные правовые нормы в действующих национальных законодательствах. Требуется их частичная унификация.
Вопрос: Вы думаете было-бы трудно найти общую почву чтобы поделиться информацией?
Ответ: По международным соглашениям мы без особых проблем обмениваемся разведывательной и иной информацией о преступлениях и правонарушениях со специальными службами зарубежных государств. В последнее время часто проходят совместные совещания, семинары и конференции наших сотрудников с сотрудниками FBI (USA).
Вопрос: Вы думаете что боязнь утери национального суверенитета –непреодолимое препятствие?
Ответ: Обмен информацией на основе двухстороннего или многостороннего Договора (юридического акта) не опасен для национального суверенитета.
Спасибо за вопросы. Были рады Вам помочь.
С уважением, ...

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Foreign Relations Law (U.S.)

- "It is universally recognized, as a corollary of state sovereignty, that officials in one state may not exercise their functions in the territory of another state without the latter's consent."
S4 Plausible Deniability

• Maze-like architecture of Internet
  – Investigations often find only hacked box
• Smart hackers route attacks through ...
  – Poor diplomatic relations
  – No law enforcement cooperation
• The problem of the last hop, retaliation
S5 Non-State Actors

- Nation-states like to control international conflict
- Transnational subcultures spontaneously coalesce online, influence political agendas
  - Report to no chain-of-command
- Globalization, Net aid in following, shaping events
- Challenge for national security leadership:
  - Could it spin delicate diplomacy out of control?
The Chinese hackers advocate the freedom
We merely make the safe examination
Invades the Personnel
江南剑书生, FraNyIsE, Shuog, LuSang, HnBin, PlioY, XoKu
'UFO Hacker' Tells What He Found

Nigel Watson 06.21.06

The search for proof of the existence of UFOs landed Gary McKinnon in a world trouble.

After allegedly hacking into NASA websites -- where he says he found images of what looked like extraterrestrial spaceships -- the 40-year-old Briton faces extradition to the United States from his North London home. If convicted, McKinnon could receive a 70-year prison term and up to $2 million in fines.
The New York Times

Monks Are Silenced, and for Now, the Web Is, Too

October 4, 2007

It was about as simple and uncomplicated as shooting demonstrators in the streets. Embarrassed by smuggled video and photographs that showed their people rising up against them, the generals who run Myanmar simply switched off the Internet.
OpenNet

**Figure 1. Timeline of Events, Aug. 19-Oct. 13, 2007**

- Demonstrations begin (Aug 19)
- Demonstrations reach 100,000 protesters (Sep 23)
- Violent crackdown begins (Sep 28)
- Government institutes complete Internet shutdown (Sep 29)
- Internet up at night (Oct 4)
- Internet up mid-day and at night (Oct 9)
- Internet begins to come back up full-time (Oct 13)

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Internal Security First

- The East German dilemma
- Computers to the Rescue
  - Processing power, databases, automated analysis, decryption, speech recognition, transcription, Artificial Intelligence, neural networks

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
## World Press Freedom Index 2006 - The rankings

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Finland</td>
<td>0,50</td>
</tr>
<tr>
<td>-</td>
<td>Iceland</td>
<td>0,50</td>
</tr>
<tr>
<td>-</td>
<td>Ireland</td>
<td>0,50</td>
</tr>
<tr>
<td>-</td>
<td>Netherlands</td>
<td>0,50</td>
</tr>
<tr>
<td>5</td>
<td>Czech Rep</td>
<td>73,50</td>
</tr>
<tr>
<td>6</td>
<td>Estonia</td>
<td>75,00</td>
</tr>
<tr>
<td>-</td>
<td>Norway</td>
<td>76,00</td>
</tr>
<tr>
<td>8</td>
<td>Slovakia</td>
<td>90,88</td>
</tr>
<tr>
<td>-</td>
<td>Switzerland</td>
<td>94,00</td>
</tr>
<tr>
<td>10</td>
<td>Hungary</td>
<td>94,75</td>
</tr>
<tr>
<td></td>
<td></td>
<td>95,00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>97,50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>98,50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>109,00</td>
</tr>
</tbody>
</table>
LIBERTY WAITS ON YOUR FINGERS –
KEEP ON BLOGGING!
http://eff.org/bloggers/

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Cyber Warfare Tactics

1. Espionage
2. Propaganda
3. Denial-of-Service (DoS)
4. Data modification
5. Infrastructure manipulation
T1 Espionage

- Second oldest profession, v 2.0
  - Elegance of remote intelligence collection
- Old vulnerability, new advantage?
  - Convergence, speed, practical crypto, steg, OSINT
- Danger not in data theft, but giving to “handler”
  - Old methods: Brush passes, car tosses, dead drops
  - New methods *virtually* the same
- Targeted collection: how would you fare?
Internet: Swedish Hacker Accesses Embassy E-Mail Accounts

De Chine, les « hackers rouges » ciblent les sites Internet de pays rivaux

NZ government computers 'hacked'

Hacking into the French state

Industrious Iranian Industrial Espionage in Germany

China accused of hacking into heart of Merkel administration

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
The New Espionage

- Universal media and intelligence gathering
  - Binoculars, satellites, mass media, NMAP?
  - Territorial sovereignty not violated
  - Metadata and reading between the lines
  - Picture taking, not physical invasion … right?
  - If indefensible, normally not espionage!

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
T2 Propaganda

• Easy, cheap, quick, safe, powerful
  – Audience is the world
  – Drop behind enemy lines
• Does not need to be true
• Recruitment, fund raising, hacktivism
  – Censored information replaced in seconds
• Tech expanding rapidly (multimedia, Skype, etc)
• Appearance of technical prowess

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Zone-H Stats

By attack reason:

- Heh...just for fun! 34%
- No reason specified 18.5%
- I just want to be the best defacer 13.7%
- As a challenge 11.4%
- Patriotism 10.5%
- Political reasons 10.1%
- Revenge against that website 1.8%
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Ne Mutlu Turkum Diyene

Powered By Blow II

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Message to the American People

In the name of God, the Compassionate, the Merciful O, Almighty God, bestow upon humanity the perfect human being promised to all by You, and make us among his followers. Noble Americans,

Were we not faced with the activities of the US administration in this part of the world and the negative ramifications of those activities on the daily lives of our peoples, coupled

Great site, Thank you very much Dr. Ahmadinejad for standing up for the truth and for standing up to evil and as a white male in the U.S. I give my full to you your country and I send you many blessings.

Dear Dr. Ahmadinejad, Thank you for sharing your thoughts with us. I am English and have a very different way of life from yours, of course. Even though I do not observe any religion.
Ministry of Health and Child Welfare

Command Tribulation Ownz your b0x

Jesus loves you

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
T3 Denial-of-Service (DoS)

• Simple strategy
  – Deny computer resource to legitimate users
  – Most common: flood target with bogus data so it cannot respond to real requests for services/info

• Other DoS attacks
  – Physical destruction of hardware
  – Electromagnetic interference designed to destroy unshielded electronics via current or voltage surges
T4 Data Modification

- Extremely dangerous
  - Legitimate users (human or machine) may make important decisions based on maliciously altered information
- Website defacement
  - “Electronic graffiti” can carry propaganda or disinformation
- Holy Grail
  - Weapons, Command and Control (C2) systems

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
T5 Infrastructure Manipulation

- Critical infrastructures connecting to Net
- SCADA security may not be robust
- Electricity especially important
- Infrastructure in private hands
- Seized hard drives: Microstran, Autocad, etc
- White House briefed on certain 0-days
Case Study #1
Russia and Chechnya: 1994

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Professor U.Ezhiev's sons kidnapped

On the night of 9 March 2003, in Staropromislov district of the Chechen capital Grozny, the Russian servicemen kidnapped two brothers Ezhaevs - Ruslan and Arby Umalatovich. Certain details of the incident have become known today.
Push and Pull

• World Wide Web
  – Real-time, unedited news from the war front
  – Net aids in following and *shaping* current events

• Average Net user
  – More information than heads of state ten years ago
  – Increasingly important role in international conflicts

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Examples

• Most effective info not pro-Chechen but anti-Russian
  – Digital images of bloody corpses, POWs
  – Real photos and fake photos used
  – Kremlin occasionally caught off-guard

• War funds bank account in Sacramento, CA

• As tech progressed, streaming videos
  – Ambushes on Russian military convoys

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Government Reaction

• 1999: PM Vladimir Putin:
  – “we surrendered this terrain some time ago ... but now we are entering the game again.”
  – Introduction of “centralized military censorship regarding the war in the North Caucasus”
  – Sought Western help to shut down kavkaz.org
Case Study #2
NATO and Kosovo: 1999

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
• 1999: first major NATO military engagement
• First Cyber war!
  – ;)
Black Hand 1.0

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Black Hand 2.0

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Hacker Achievements

- NATO war website down, email down
  - “Line saturation” caused by “hackers in Belgrade”
- White House website defaced
  - Secret Service investigation
- Virus-infected email
  - 25 strains detected
- “Owned” U.S. Navy computer
Case Study #3
Middle East
Cyber War: 2000
חתיכה - לא לעת!

מבחין הדרוש
ליבן איינא!

הילל החשופים

על מתי?

 enumerator: israforce.net

םוכנים: ניינר

ירכון הפיות לפלפל

חתיכה

ז"ט

יתנשף

Ynet News

йтиין

שתלה פעילה

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

Plate

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכ

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דרכ

חתיכה

יתנשף

_plate-

ץ"ג

יתני

牒
c

דруч
CCDCOE

www.hizbulla.org: October 25, 2000

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Attacked by m0sad: 67 of which 54 are single IP and 13 mass defacements

Legend:
- H - Homepage defacement
- M - Mass defacement (click to view all defacements of this IP)
- R - Redefacement (click to view all defacements of this site)
- ✫ - Special defacement

<table>
<thead>
<tr>
<th>Time</th>
<th>Attacker</th>
<th>Domain</th>
<th>OS</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001/01/03</td>
<td>m0sad</td>
<td>H sys.edu.pk</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/02</td>
<td>m0sad</td>
<td>H saaa.org</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/02</td>
<td>m0sad</td>
<td>H mustafadaas.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/02</td>
<td>m0sad</td>
<td>H spicers.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2001/01/01</td>
<td>m0sad</td>
<td>H modell.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/31</td>
<td>m0sad</td>
<td>H dpi.net.ir</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/31</td>
<td>m0sad</td>
<td>H sysnet.com.pk</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/29</td>
<td>m0sad</td>
<td>H hrep.com.pk</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/20</td>
<td>m0sad</td>
<td>H isna.net</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/19</td>
<td>m0sad</td>
<td>H iugaza.edu</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/15</td>
<td>m0sad</td>
<td>H talkislam.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/12</td>
<td>m0sad</td>
<td>✫ mfa.gov.ir</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/10</td>
<td>m0sad</td>
<td>✫ dcaauh.gov.ae</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/03</td>
<td>m0sad</td>
<td>✫ islam.gov.qa</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/12/01</td>
<td>m0sad</td>
<td>H webhosting.ajeeb.com</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/11/29</td>
<td>m0sad</td>
<td>H islamweb.net</td>
<td>Windows</td>
<td>view</td>
</tr>
<tr>
<td>2000/11/27</td>
<td>m0sad</td>
<td>H khaleej.com</td>
<td>Windows</td>
<td>view</td>
</tr>
</tbody>
</table>
Pro-Palestinian Counterattack

• Immediate, much more diverse
• Key difference: economic targets
  – Bank of Israel, e-commerce, Tel Aviv Stock Exchange
  – At least 19 countries: AIPAC, AT&T
• During 2006 Gaza fighting
  – 700 Israeli Internet domains shut down
GROUP(I):
Click HERE and Help the Resistance(I).

“You will attack…”
...these IPs:
  IP: 212.143.256.4
  IP: 212.143.256.4
- http://www.israel.com
  IP: 63.194.226.226
  IP: 194.90.202.20

and...
Bank of Israel
Tel Aviv Stock Exchange
Prime Minister’s Office
www.wizel.com

GROUP(II):
Click HERE and Help the Resistance(II).

You Will Attack:
- www.bankisrael.gov.il
  IP: 161.58.232.244
- Tel Aviv Stock Exchange(www.tase.co.il)
  IP: 192.116.46.129
- www.pmo.gov.il(Prime Ministry Office)
  IP: 147.237.72.93
- www.wizel.com
We have been forced to remove this site

The bandwidth providers to our ISP, after receiving many complaints from Zionists and their supporters in the UK, have threatened to cut off our internet connection if this site was not removed. We have therefore removed this site in order to keep the rest of ummah.com online.

Most sincere apologies,

The ummah.com team
www.ummah.com/unity

- Due to complaints, moved and renamed:
  - http://defend.unity-news.com
  - http://members.tripod.com/irsa2003
  - http://members.tripod.com/irsa2004

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Case Study #4

Sino-American
“Patriotic Hacker War”: 2001
April 26, 2001: FBI Advisory

“Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems … Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC…”

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Downed EP-3 on Hainan Island

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Critical Infrastructure Attack

• FBI investigated a Honker Union of China (HUC), 17-day hack of a California electric power grid test network
  – Widely dismissed as media hype
• 2007: CIA informed industry leaders that a tangible hacker threat to critical infrastructure is no longer theoretical
Case Study #5
Estonia: 2007
The North Atlantic Treaty
Washington DC, 4 April 1949

- Article 5: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all ... each of them ... will assist the Party or Parties so attacked by taking forthwith ... such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
Red Square, 1945
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Tallinn, Estonia
### Ethnic Composition of Estonia

<table>
<thead>
<tr>
<th>Ethnicity</th>
<th>Population</th>
<th>% of total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estonian</td>
<td>921,062</td>
<td>68.6</td>
</tr>
<tr>
<td>Russian</td>
<td>344,280</td>
<td>25.6</td>
</tr>
<tr>
<td>Ukrainian</td>
<td>28,158</td>
<td>2.1</td>
</tr>
<tr>
<td>Belarusian</td>
<td>16,134</td>
<td>1.2</td>
</tr>
<tr>
<td>Finn</td>
<td>11,035</td>
<td>0.8</td>
</tr>
</tbody>
</table>
The Russian Border
Relocation: April 26, 2007

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
На 9-е МАЯ планируется повтор данной акции!
Не дай унизить своих соотечественников, отомсти за издевательства !!!
@ адреса eSSтонских депутатов

Программа для рассылки писем
(пароль на RAR: nmm )

Нажми (пуск -> выполнять -> cmd)
введи ping -n 5000 -l 10000 эSSтонский_сайт -t и жми ENTER ВСЕ !!! Твои пламенные приветы полетели...
пример: ping -n 5000 -l 1000 www.riik.ee -t
Это 3 элементарных действия, после которых многие эстонские сайты просто перестанут работать!!!
Или вот .BAT файл, который в автоматическом режиме последовательно пингует эстонские DNS и MAIL сервера. Цикл бесконечен :)
Скопировать (красным) нижеприведённый текст, вставить в блокнот и сохранить как priveteSStoria.BAT (название можно любое) файл
(ты можешь сам добавлять адреса )
May 9: Victory Day
• «Премьер-министр просит прощения! Премьер-министр Эстонии и эстонское правительство просят прощения у всего русского населения Эстонии и берут на себя обязательства по возвращению памятника бронзовому солдату на место.»

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Estonian Retaliation?

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
NATO: Dawn of Cyber

- 1999 Washington Summit (new “Strategic Concept”)
  - No mention of cyber
- 2002 Prague Summit:
  - “strengthen ... to defend against cyber attacks”
- 2004 Istanbul Summit:
  - No mention of cyber
- 2006 Riga Summit:
  - “protect information systems ... against cyber attacks”
  - “develop a NATO Network Enabled Capability”
Centre of Excellence, Tallinn
Strategic Thoughts

• Nation-states lose some control over conflict
• Geopolitical analysis required
  – Cyber conflict mirrors fighting on ground
• Attribution and the false flag
  – Concept: People’s War
• Is national security at risk?
  – As with WMD, defense strategies unclear
  – As with terrorism, success in media hype
Tactical Thoughts

• Assume Breach!
• Collection/transmission of evidence
• Asymmetric advantage works both ways
• Set realistic goals
• Focus on core problems
• Blend art and science
• w/o competent ctrmeasures, much worse...

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
The New York Times

July 1, 2008

Hackers Tag Lithuanian Web Sites With Soviet Symbols

By SARA RHODIN

MOSCOW — Hackers attacked about 300 Web sites in Lithuania over the weekend, with Soviet symbols and anti-Lithuanian slogans, officials said Monday.
Cyberwar and real war collide in Georgia

By John Markoff

Published: August 13, 2008

Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace.

Jose Nazario of Arbor Networks in Lexington noticed a stream of data directed at Georgian government sites with the message: "win+love+in+Rusia."

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
The Future is Unknown

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
But It Begins Today

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Cyberspace and the Changing Nature of Warfare

Kenneth Geers

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia