Piracy, Privateering

... and the creation of a new Navy

SOURCE Dublin 2013 Keynote
thomas.dullien@googlemail.com

Strange title for a talk ?

Keynote talks are not supposed to be technical

I don't know much outside of technical stuff

My approach: Sit back and reflect about where we're headed. Turn these musings into a talk.

My views

Former IRC kid in the 90's

Reverse engineering since '97 or so

Vuln-dev etc. since '99

Been around for a while, seen a few things

"building a new Navy"

Television Guy: "Isn't hiring 1000 computer experts terribly expensive ?"

Dave Aitel: "On the one hand, yes - but not really if you are building a new Navy, which is what is happening here."

Wait, what ?

What does hiring hackers have in common with building a Navy ?

Waterways

The cheapest way to transport physical goods is shipping

Control of shipping lanes is control of the flow of goods - and hence money

The internet

The cheapest way to transport bits is the internet

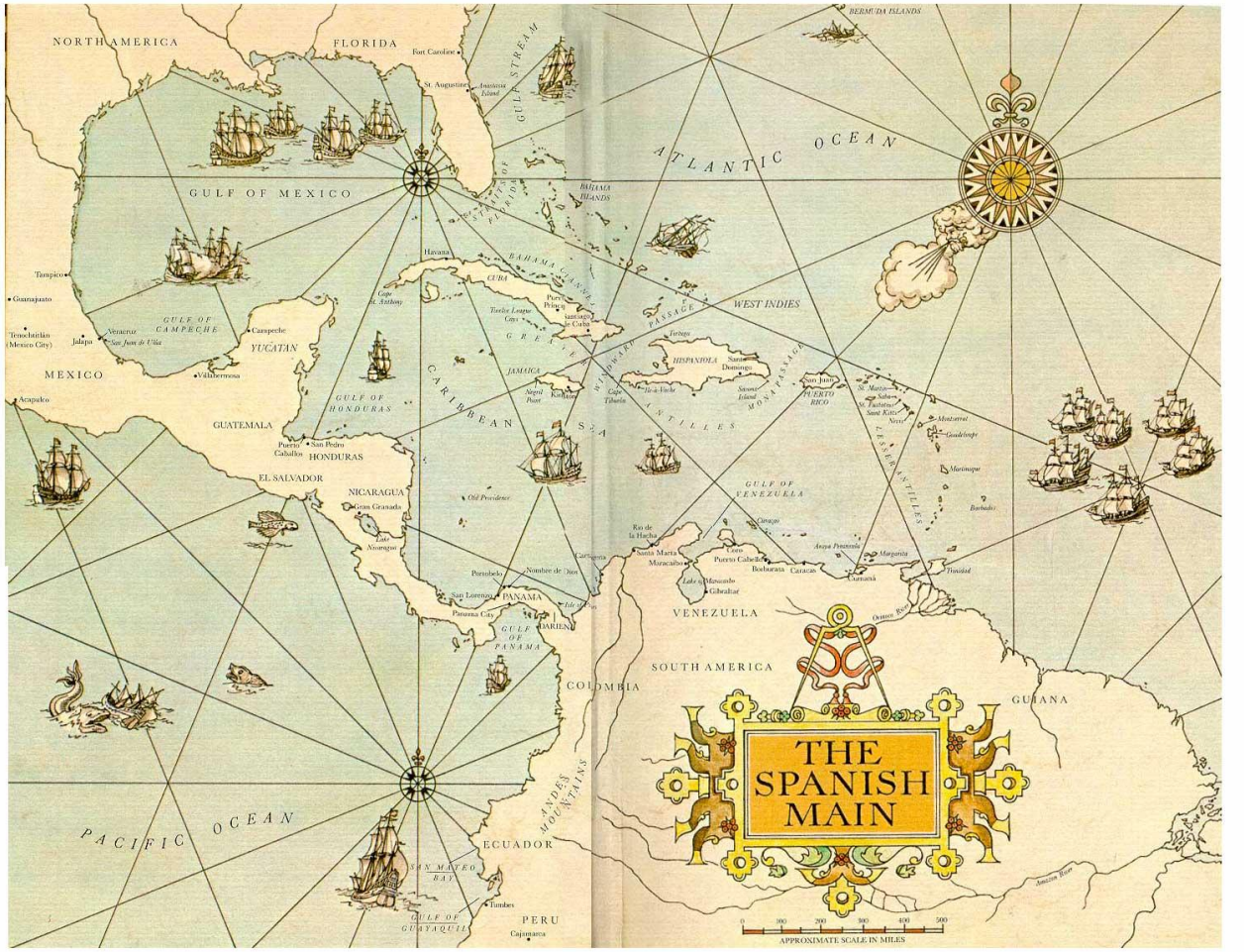
Control of the network means control of transport lanes for "digital goods"

Thesis of this talk

We witnessed, during our lifetimes, the digital equivalent of the *"La conquista"* - but instead of a new continent that was discovered, this new continent was *built*.

As the world's trade flows are becoming dependent on computers, we will see the rise of "new Navies".

The Spanish Main



History: 1500's

Spain is the dominant superpower

Discovery of the new world - but until the 1520's, it's a backwater

With the 1520's, silver mining in Mexico starts

It isn't until the 1570's that other countries catch on (more later)

History (pre-2000)

Pre-2000-hackers are mostly explorers - not law-abiding, but not primarily goal/profit-driven

Trade volume on the internet is low

With the first dot-com boom, trade rises

With trade come opportunities for profit, both legal and illegal

The internet pre-2000

Nearly complete legal vacuum

Not important enough to divert resources for policing it

Law of the strongest - but on a very low level

Situation in 2001

15 year-old Canadian teens controlled then-huge DDoS networks

Networks presumably controlled by the authors of TFN and Stacheldraht at the time: Much larger

Situation in 2001

"Internet-ending" 0day routinely in the hands of a few teenagers

Significant percentage of the Internet compromised by amateurs

Relatively little of "serious" nature happened: Not much money yet, hackers didn't know what to do with their warez

Similarities

The pre-2000 internet is very similar to early 1500's Spanish Main

Frontier area, but hardly anyone has recognized the future economic importance

Lawless zone, but not by structure - by choice (e.g. disinterest)

Boucanier (Buccaneer)

Non-spanish, illicit settlers on Hispaniola

Name derives from "boucan", a wooden grill used for smoking meat

Traded in smoked meat initially - until they figured out that they can raid Spanish ships

History: 1600's

Spain vs France, vs Britain, vs Holland

France, Britain, and Holland draw on existing Boucanier community to ramp up sea power

Transformation: Small-scale pirates transform into large-scale privateering outfits

At the same time: Ramp-up of regular Navies

Hackers

Unintended, illicit settlers on the early internet

Traded in ways of exploring more of the new world

Some identified ways of profiting off their exploration, sometimes criminal, but generally small-scale

2001-2013

Rapid economic and societal change through widespread adoption of the Internet

Rise of Internet Giants: Amazon, Google, Facebook

Expanded defense spending after 9-11

Rise of privateering

Governments realize importance of the Internet

Large powers draw on existing Hacker community to ramp up network capability

Hacker community splits up into interesting fragments

Parallel ramp-up of surveillance / monitoring

Fragments

Navy: Full-on government employment

Privateers: Hackers working as private industry, but backed by government policies

Fragments

Mercenaries to merchants: Hackers working to protect the new trade routes / ports for internet giants

Piracy: Enterprises without government or commercial backing

"Letters of Marque"

Allowed privateers to attack ships of other nations independently

Often "in retribution for losses suffered"

New York Times, two days ago:

"As Chinese Leader's Visit Nears, U.S. Is Urged to Allow Counterattacks on Hackers"

Privateers

Clearly, there's a lobby for allowing privateering

Government-backed, but private enterprise

Mixing military and economic objectives

Francis Drake

Financed his raids on the Spanish main through third-party investors

Britain could not openly support such raids without risking war with then-superpower, Spain

Among the investors was Queen Elizabeth

Francis Drake

Ridiculously profitable: First big raid yielded 50% of the annual British Crown's income from one Spanish ship

Sounds familiar ?

Will the architects behind industrial espionage operations be eventually knighted in their respective home countries ?

Is the supposed Chinese economic espionage much different from the policies Britain had toward Spain in the late 1500s ?

Piracy without home port

Most pirates that refused to align with a government, and that could not rely on a home port, were eventually executed

Piracy without home port

Wikileaks and TPB may be modern-day examples of "pirates" that did not have government backing.

Privateering risks

Henry Morgan led a raid on Porto Bello as British privateer

Plunder from that raid alone: 300m USD in today's money

British made peace with Spain, depriving him of his hobby

Privateering risks

Arrested him in April 1672, shipped him to London

His luck: War with the Dutch broke out, he was back in demand & freed

Many unemployed privateers turned to piracy, and were then prosecuted & killed

Other amusing similarities

The then-superpower Spain used privateers sparingly, and mostly relied on regular troops

The challengers to Spanish hegemony used privateers freely

Compare: "Western" approach to computer attacks vs. presumed Russian/Chinese approach

Future: Short-term

Short-term: The next 10 years

"There are only two levels of difficulty in mathematics: Trivial and not understood"

(Alan T. Huckleberry)

"There are only two sorts of source code in IT: Trivial and code execution for the attacker"

Future: Short-term

Right model to think about security?

Any opening of any document is equivalent to granting the attacker the ability to run arbitrary code

Sandbox things tightly

Future: Short-term

Will sandboxing become sufficiently robust in the next 10 years to obsolete most bugs ?

Transitive trust is the silent killer

Compromise all large vendors *now* and steal their update signing keys

Future: History

Frontal, sea-side assaults on ports became impossible eventually

Attacks on big ports in the Spanish Main happened mostly overland

Why exploit if you can update ?

The future

Small trading outposts are abandoned, commerce is moved into defendable large ports

Specialized convois transport goods under protection

"Cloud"

The future

Eventually, Navies take over

Navies perform tight surveillance of sea lanes and ensure safety for commerce

Threats of conventional war & economic damage forces governments to rein in privateering

The future

This can take a long time

Navy-style surveillance will probably mean full-packet capture for the internet

~20 Exabyte / month - Utah Datacenter: 5 Zetabyte storage

The future

This can be expensive

Pompey eradicated piracy in the mediterranean in Roman times

Rome dedicated 50% of their entire defense budget to this task (albeit only for a few monts)

The future

"Pax Britannica", but under the aegis of a different superpower ?

Which one ?

Any questions ?