Cyber-Warfare

New Canaan Exchange Club
Paul A. Strassmann, July 18, 2017

Notifications About Russian Information Warfare

NCCIC

Federal Bureau of Investigation

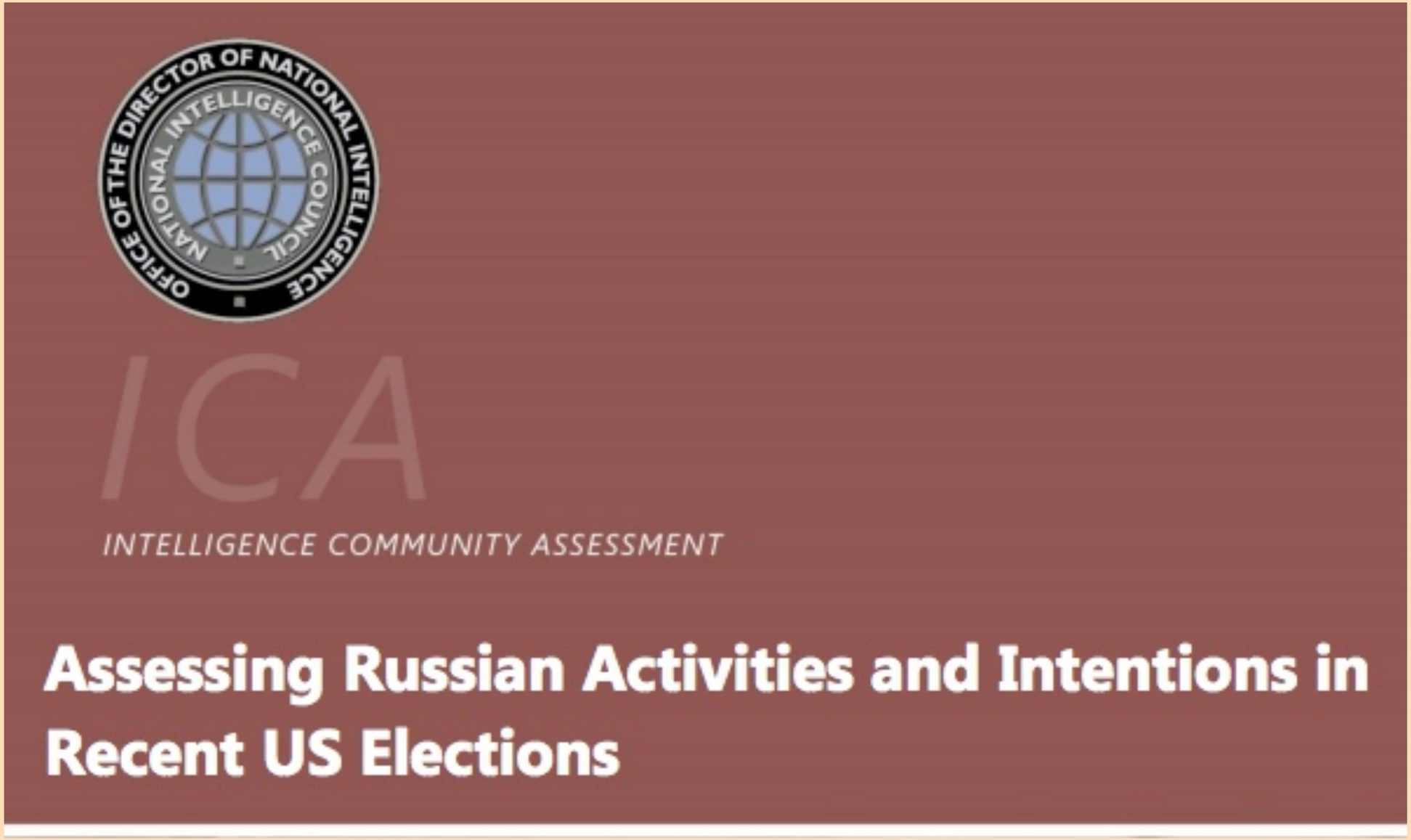
JOINT ANALYSIS REPORT

DISCLAIMER: *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296 **December 29, 2016**

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Intelligence Assessments



Russian Cyber-Intrusion Agents – 12/2016

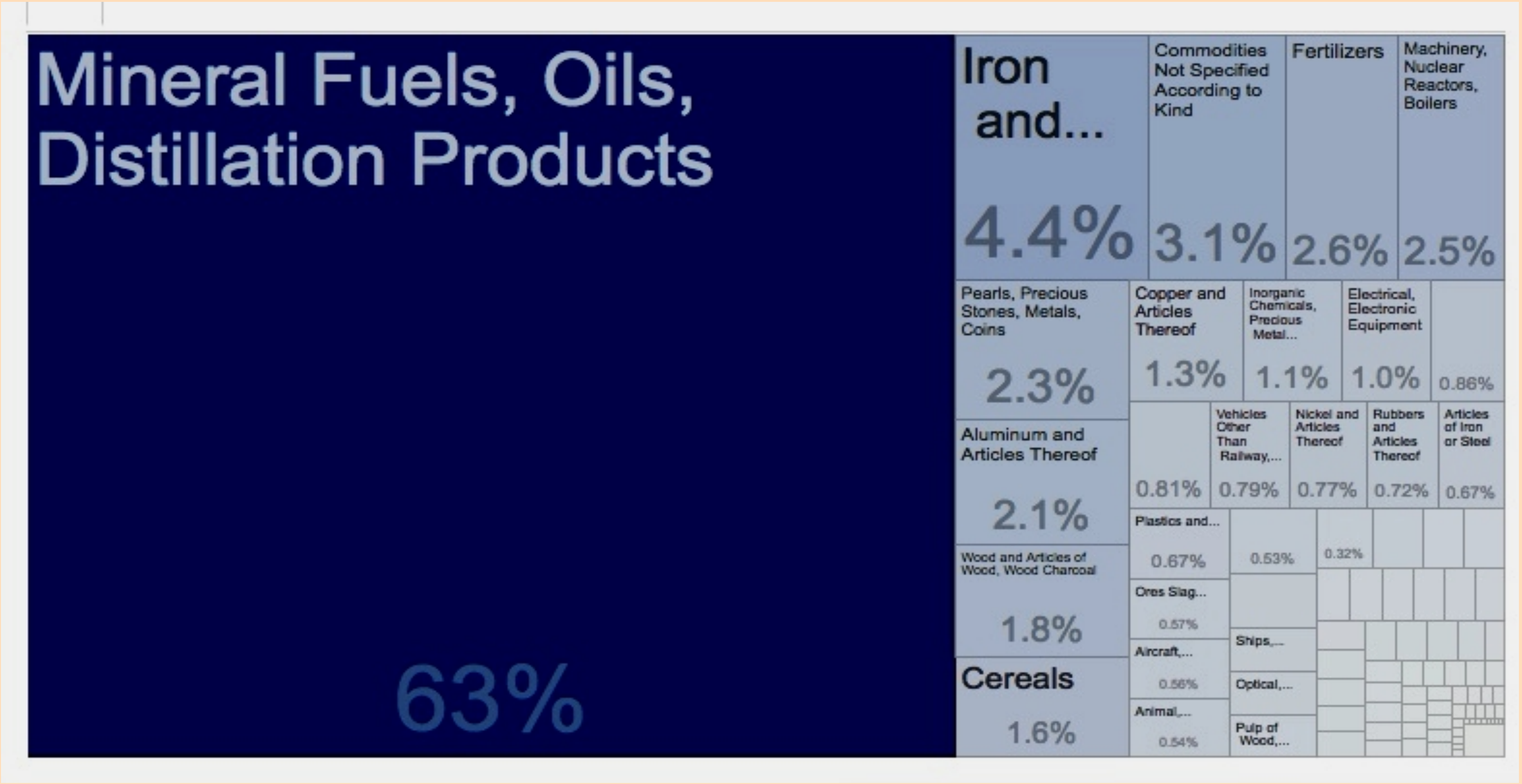
APT29
Agent.btz
BlackEnergy V3
BlackEnergy2 APT
CakeDuke
Carberp
CHOPSTICK
CloudDuke
CORESHEL
COZYBEAR
COZYCAR
COZYDUKE
CrouchingYeti

DIONIS
Dragonfly
Energetic Bear
EVILTOSS
Fancy Bear
GeminiDuke
GREY CLOUD
HammerDuke
HAMMERTOSS
Havex
MiniDionis
.
.
Etc.

Russia is a Relatively Poor Country, With Large Defense Spending

Country Name	Russian Federation	Russian Federation	Russian Federation	Russian Federation	United States	United States	United States	United States
Year	GDP (constant 2010 US$)	GDP growth (annual %)	GDP per capita (constant 2010	Military expenditure (% of GDP)	GDP (constant 2010 US$)	GDP growth (annual %)	GDP per capita (constant 2010	Military expenditure (% of GDP)
2015	$1,631,640,000,000	-2.8	$11,145	4.9	$16,597,400,000,000	2.6	$51,638	3.3

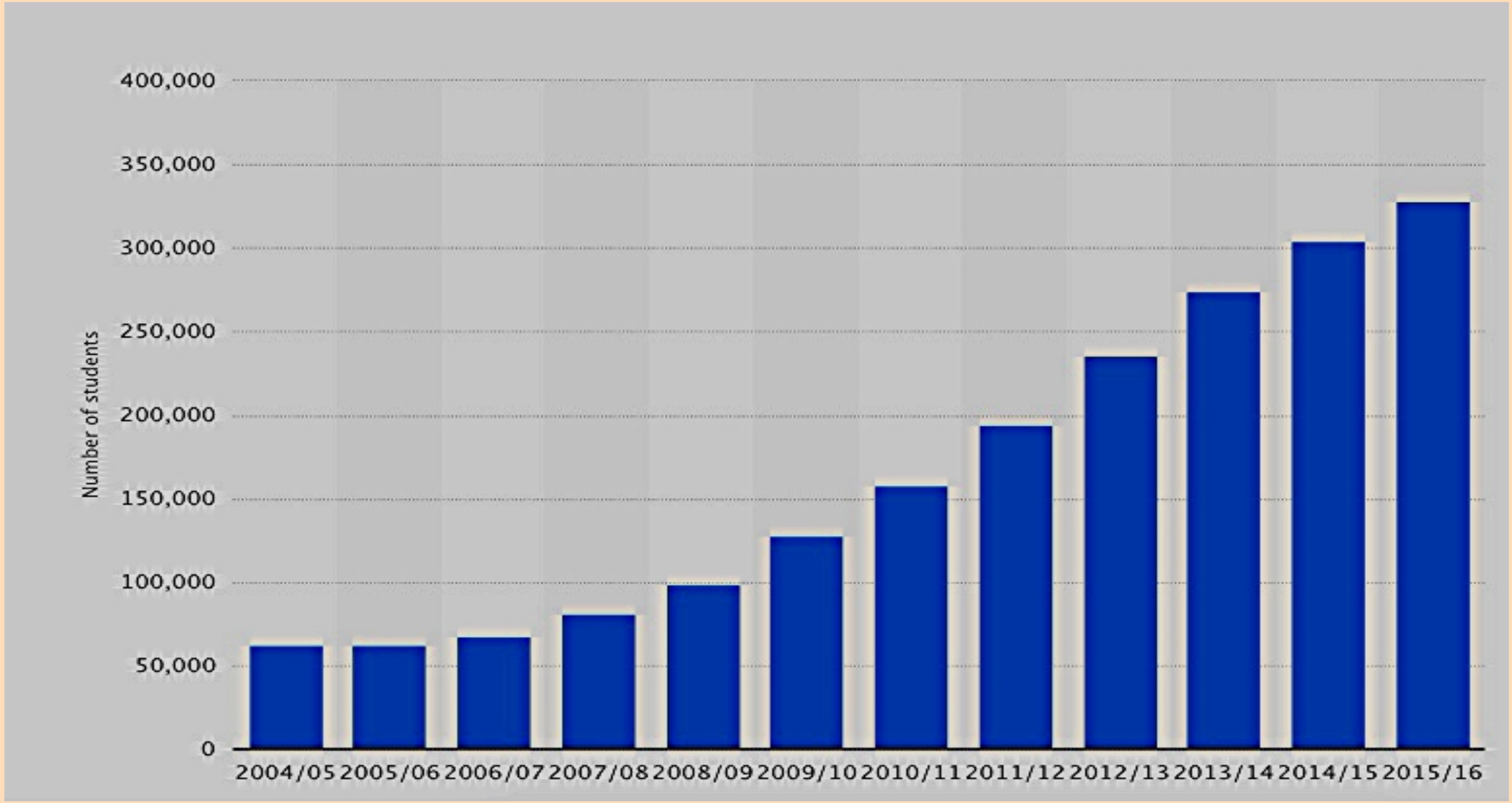
Russia is a Supplier of Raw Materials, Not an Industrial Competitor



2016 exports from the Russian Federation - % of total

China Also Involved in Cyber Espionage

Number of Chinese Students in the USA



Estimated Costs of Defenses

- Global cost of cyber incidents grows from $3 trillion in 2015 to $6 trillion by 2021.
- Global GDP (2016) is $76.6 trillion.
- Cyber/GDP appx. 5%

What is Cyber Warfare

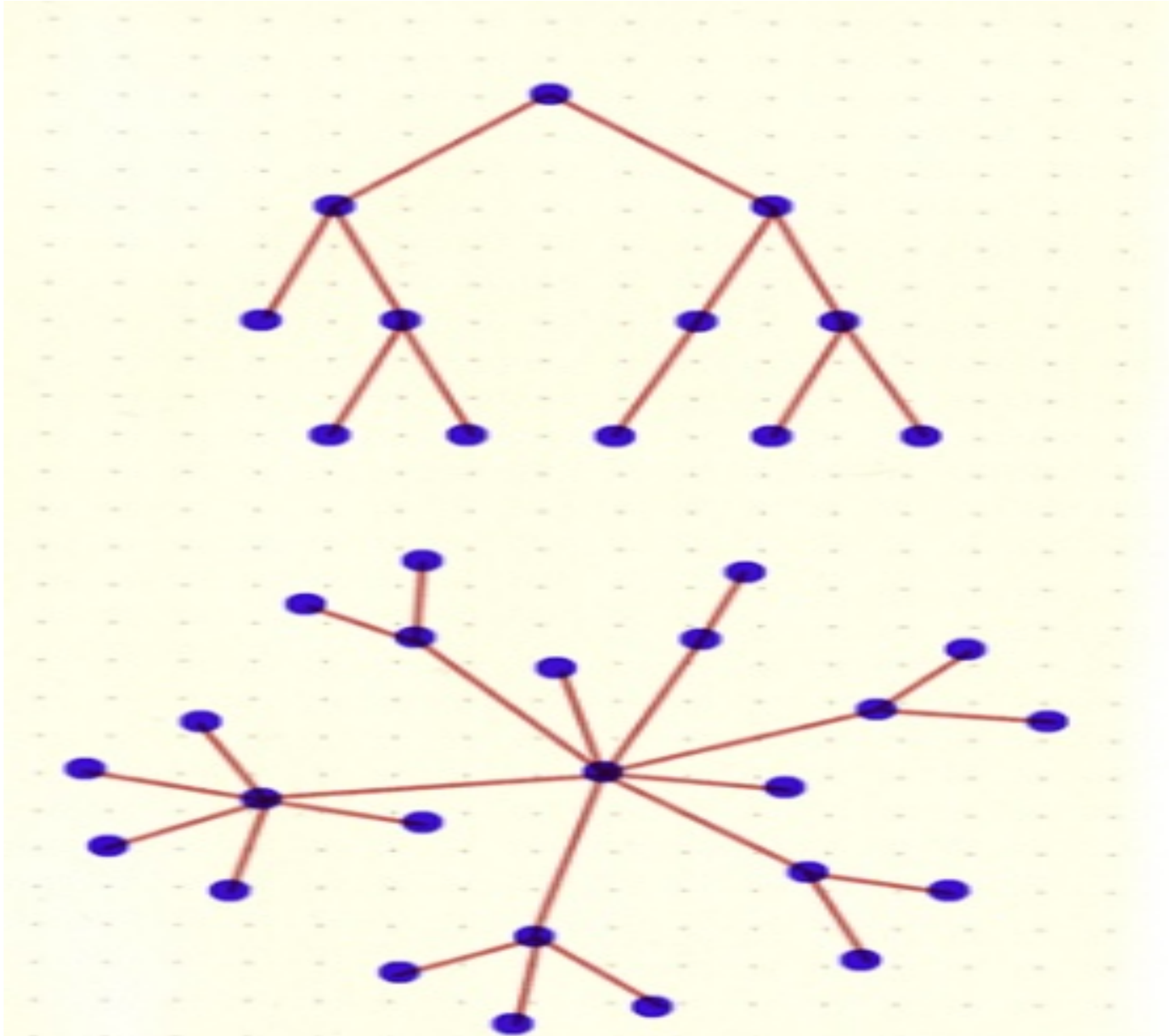
Attacks Received: Millions/day. Must counter all.

***Attacker costs: close to zero**.*

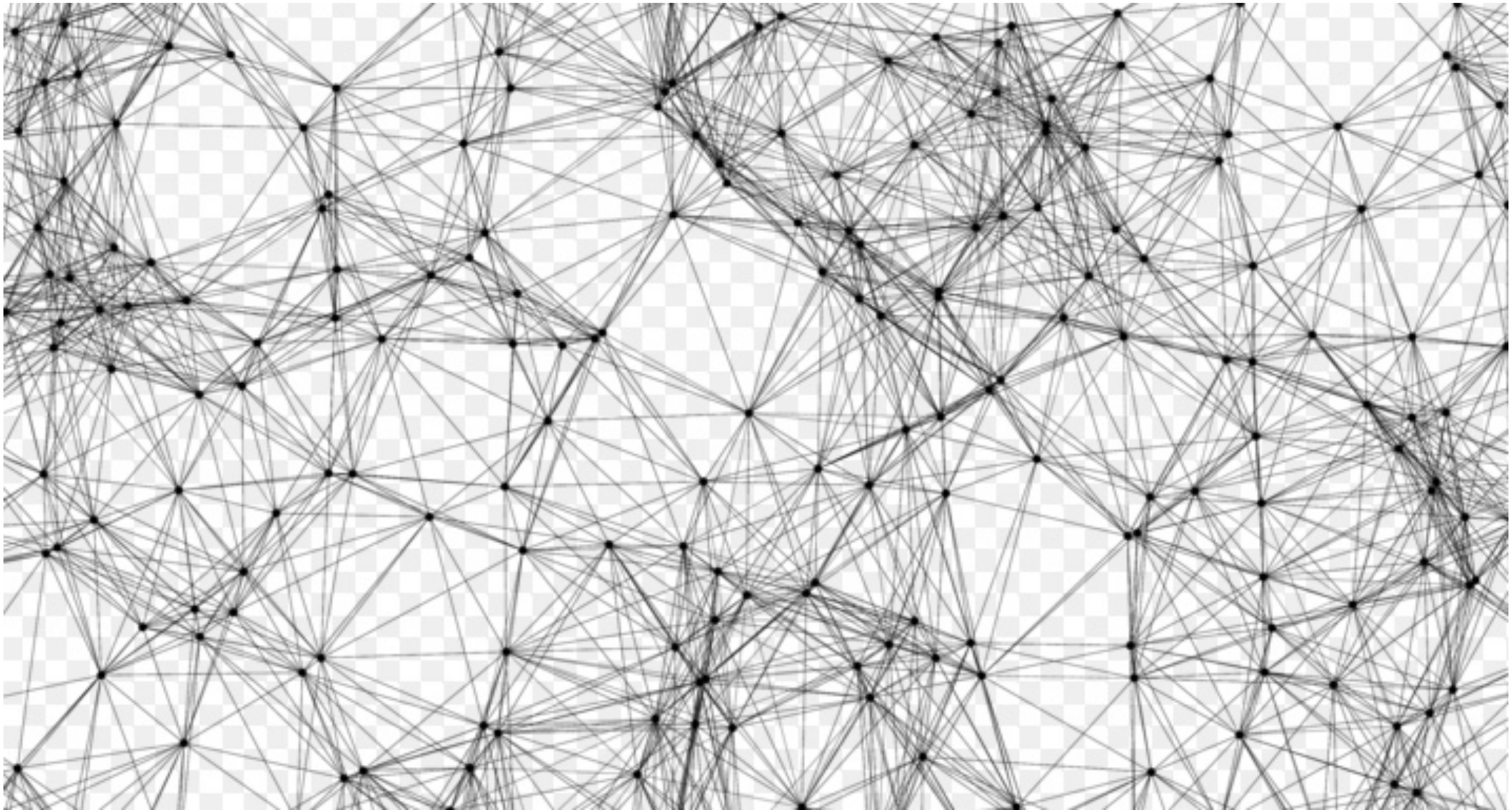
Defenses: Very Few. Must intercept every one.

Defender costs: Estimated at >5% of GNP.

Defending Simple Networks



Present Networks Can Be Hacked



Billions Interconnections on Global Internet

What Are Causes of Vulnerability?

- System design flaws.
- Errors in computer code.
- Unauthorized access privileges.

List of Critical Vulnerabilities (CVE >9)

Security Vulnerabilities Published In July 2017 (CVSS score >= 9)

2017 : January February March April May June July CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level
1	CVE-2017-1000082	20			2017-07-07	2017-07-12	10.0	Admin
systemd v233 and earlier fails to safely parse usernames starting with a numeric digit (e.g. "0day"), running the service in qu								
2	CVE-2017-11176	416		DoS	2017-07-11	2017-07-14	10.0	None
The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry log to cause a denial of service (use-after-free) or possibly have unspecified other impact.								
3	CVE-2017-10994	123		Exec Code	2017-07-07	2017-07-13	9.3	None
Foxit Reader before 8.3.1 and PhantomPDF before 8.3.1 have an Arbitrary Write vulnerability, which allows remote attackers								
4	CVE-2017-10921	264		DoS Mem. Corr.	2017-07-04	2017-07-10	10.0	None
The grant-table feature in Xen through 4.8.x does not ensure sufficient type counts for a GNTMAP_device_map and GNTMAP_ of service (count mismanagement and memory corruption) or obtain privileged host OS access, aka XSA-224 bug 2.								
5	CVE-2017-10920	264		DoS Mem. Corr.	2017-07-04	2017-07-10	10.0	None
The grant-table feature in Xen through 4.8.x mishandles a GNTMAP_device_map and GNTMAP_host_map mapping, when follo OS users to cause a denial of service (count mismanagement and memory corruption) or obtain privileged host OS access, ak								
6	CVE-2017-10918	20			2017-07-04	2017-07-10	10.0	None
Xen through 4.8.x does not validate memory allocations during certain P2M operations, which allows guest OS users to obtain								
7	CVE-2017-10917	476		DoS +Info	2017-07-04	2017-07-10	9.4	None
Xen through 4.8.x does not validate the port numbers of polled event channel ports, which allows guest OS users to cause a d possibly obtain sensitive information, aka XSA-221.								

Common Vulnerability Ratings for Microsoft

Latest Scored Vulns

Showing some of the latest 20 scored vulnerabilities from the NVD, updated once per hour.

Vuln ID & Summary	CVSS Severity
CVE-2017-8607 — Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the conte... read more **Published:** July 11, 2017; 05:29:02 PM -04:00	*V3:* 7.5 HIGH *V2:* 7.6 HIGH
CVE-2017-8606 — Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the conte... read more **Published:** July 11, 2017; 05:29:02 PM -04:00	*V3:* 7.5 HIGH *V2:* 7.6 HIGH
CVE-2017-8605 — Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Mi... read more	*V3:* 7.5 HIGH *V2:* 7.6 HIGH

Bug Bounty Awards

- Bug bounty programs offer compensation for reporting bugs pertaining to security exploits and vulnerabilities.
- These programs allow developers to discover and resolve bugs before the public is aware, e.g. Zero Day Exploits.
- Bug bounty programs have been implemented by Mozilla, Facebook, Yahoo!, Google, Reddit and Microsoft.
- The "Hack the Pentagon" program ran for a month. Over 1,400 people submitted 138 unique bugs.

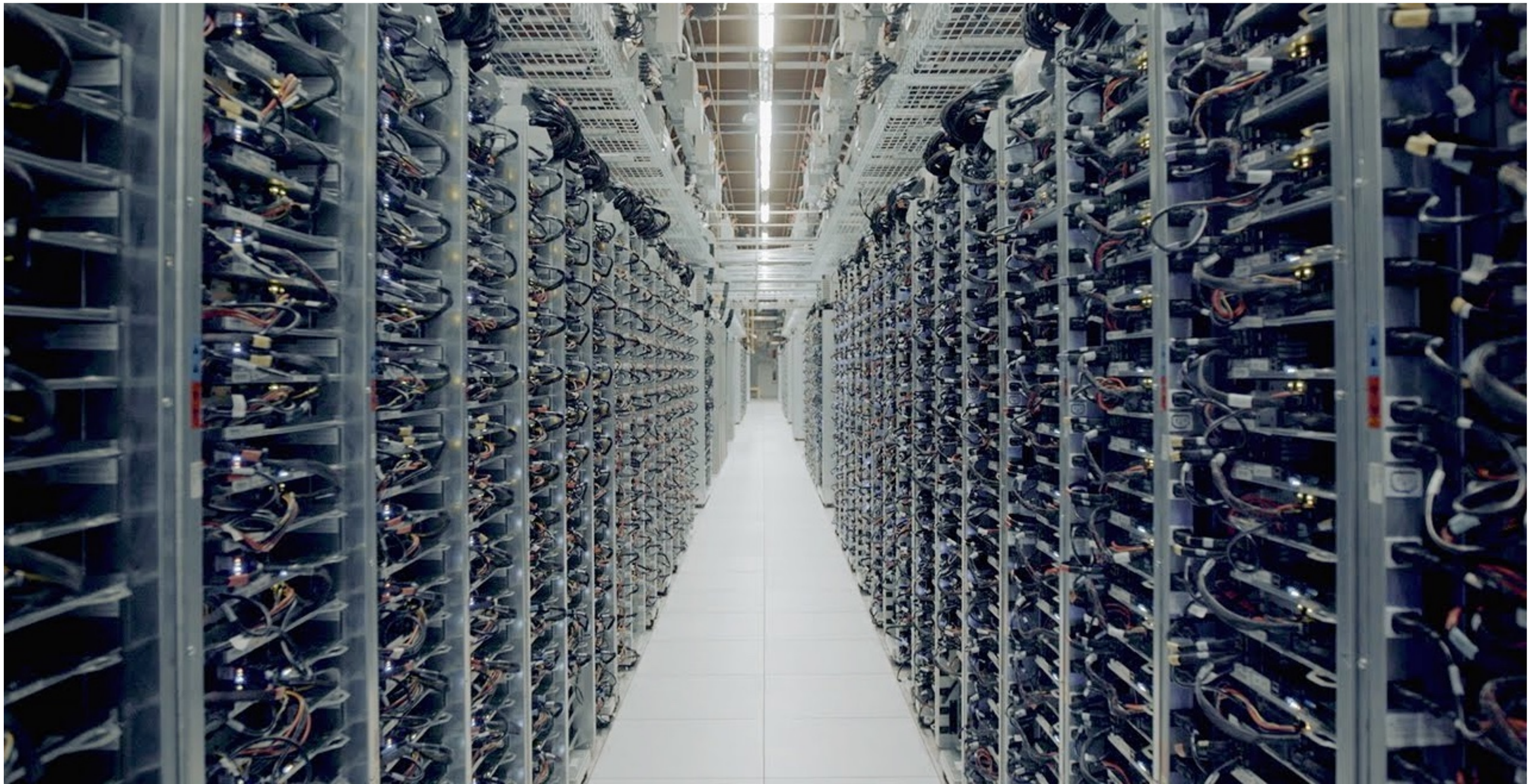
What Do Cyber Defenders Protect?

Potential destinations of cyber attack: >200 million.

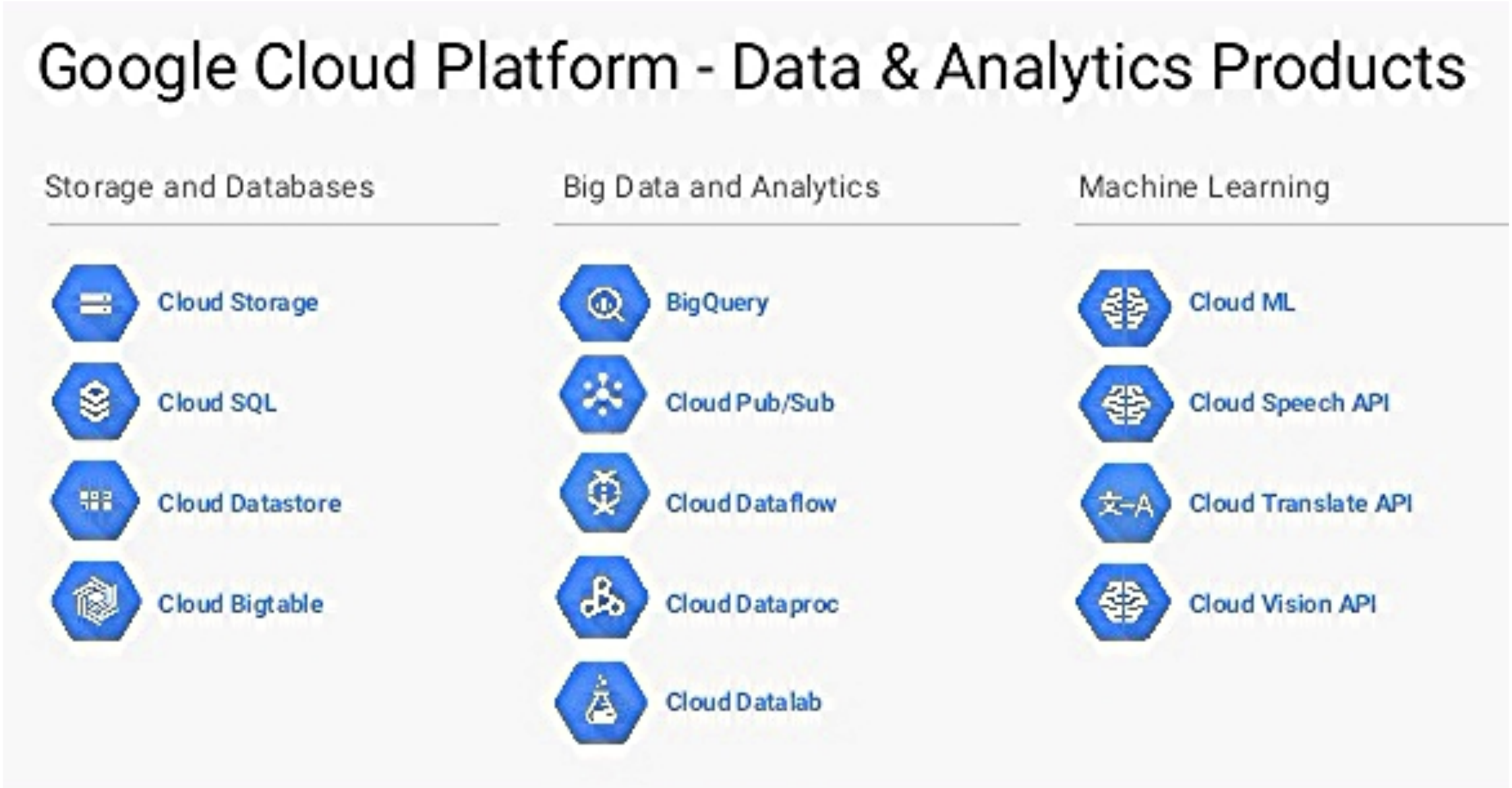
Potential paths for cyber attack: > 200 trillion.

Protection: Operate Multiple Data Centers

Secure Data Centers Cost >$1 billion



Offer Secure Software



Hacker July 22-27, 2017 Meeting

15,000+ Attendance at 2016 Black Hat Conference

Black Hat Continues to Break Records with Largest USA Show in 19-Year History

World's Leading Information Security Event Celebrates New Milestones in Attendance Alongside Most Robust Schedule in Show's History

Black Hat Arsenal offers demonstration of tools.
Features 80 tools.

Sponsors and Locations of 2016 Black Hat Conference

FireEye, Forcepoint, Hewlett Packard Enterprise, LogRhythm, Qualys, RSA, Tenable Network Security, AlienVault, Carbon Black, Cisco, Citrix Systems, CrowdStrike, Cylance, Digital Guardian, Fidelis Cybersecurity, Fortinet, Lockheed Martin Corporation, Palo Alto Networks, Symantec, Webroot, CloudPassage, Code42 Software, Core Security, Dark Matter, F5 Networks, IBM, iboss Cybersecurity, Optiv Security, Proofpoint, Inc., Raytheon Foreground Security, SentinelOne and Tripwire.

Black Hat Europe 2016, London, England, November 1-4, 2016
Black Hat Asia 2017, Singapore, March 28-31, 2017
Black Hat USA 2017, Las Vegas, NV, July 22-27, 2017

Zero Day at Black Hat

Day Zero offers attendees a comprehensive overview of all the programs, content, and special features available at Black Hat. Before diving into a jam-packed two days of hacks and research, hear from Black Hat Review Board members on a broad range of topics; from the story of Black Hat's creation, to building a content roadmap, to how to submit the perfect talk, to insider recommendations on this years can't-miss Briefings and Arsenal tools. Experts will share their views, memories, and intel to prepare you for what's in store.

DEFCON Hacking Conference, July 27 to July 30, 2017

DEF CON – 2016 Attendance of 22,000

- DEF CON is the world's largest hacking conference.
- Hackers, IT professionals and security firms discuss cutting edge research.
- Includes security security professionals, journalists, lawyers, federal government employees, security researchers, students, and active hackers.

What to Do: Convert to Managed “Cloud” Computing Services

- Place applications on secure cloud services.
- Own and operate secure data centers
- Use only secured infrastructure software.

Findings

- Cyber-warfare is an existential threat.
- Current networks cannot be defended.
- Increase cyber defense budget to 20% of IT.

- Strassmann IDC papers

- IT Security: Password Policy and Management DC Study Available ($), March 2016
- Dealing with Cyberextortion IDC Study Available ($), May 2015
- Fundamental Elements of Effective Cyberdefense IDC Study Available ($), April 2015
- Countering Cyberespionage IDC Study Available ($), April 2015
- U.S. Government Organizations Supporting Defense Against Cyberthreats IDC Study Available ($), March 2015
- Participation in Cyberthreat Information Sharing Centers IDC Study Available ($), March 2015
- Director's Oversight of Cyberthreat Protection IDC Study Available ($), February 2015
- The CIO's Role in Protecting the Enterprise from Cyberattacks IDC Study Available ($), February 2015
- Leadership Guide — Looking to Cloud Networks for Cybersecurity IDC Study Available ($), December 2014
- Leadership Guide — Partnerships for Sharing About Cyberthreats IDC Study Available ($), December 2014
- Leadership Guide — Detecting Hidden Malware IDC Study Available ($), November 2014
- Role of the National Vulnerability Database in Choosing Cyberprotection Vendors IDC Study Available ($), October 2014
- Security of Public Cloud Services IDC Study Available ($), September 2014
- The Affordability of Cyberdefense Spending IDC Study Available ($), August 2014
- Improving Cybersecurity Infrastructure A Practical Approach IDC Study Available ($), June 2014
- The Scope of Cyberthreats IDC Study Available ($), May 2014
- Eliminating Primary Causes of Cyber Vulnerability IDC Study Available ($), May 2014
- Securing Mobile Devices for the Enterprise IDC Study Available ($), March 2014
- Defending Against Internet Incursions IDC Study Available ($), March 2014
- IDC Maturity Model: IT Security IDC Study Available ($), March 2014
- IT Security: Password Policy and Management, IDC Study Available ($), November 2013
- Executive Guide to Cybercriminals and Their Methods of Attack. IDC Study Available ($), September 2013
- The Executive Guide to Protecting Platform-as-a-Service Computing, IDC Study Available ($), September 2013
- Using Big Data for Enterprise Security, IDC Study Available ($), August 2013
- The Executive Guide to Distributed Denial of Service, IDC Study Available ($), July 2013
- Executive Guide to Cyberthreats. IDC Study Available ($), July 2013
- IDC Warned about a Snowden-Like Event. IDC Insights, June 2013
- The Executive Role in Cyber-Regulations. IDC Study Available ($), June 2013
- Countering Software Robots, IDC Study Available ($), May 2013
- Insider Theft of Intellectual Property, IDC Study Available ($), April 2013
- Top Management's Responses to Cyberattacks, IDC Study Available ($), April 2013
- Insider Threats Through IT Sabotage, IDC Study Available ($), January 2013