Timeline

Date	Type of Attack	Segment	Target	Military/Civilian/Government/Commercial Target	Origin	Impact	Intent	References
1977	Hijacking	Data Comms	ITM new broadcast (audio)	Commercial	Unknown	Audio was replaced by one which warned humankind's current path would lead to a bad future	Warning	[1]
1985	Hijacking	Data Comms	State-run television broadcasts in Torun	Government	Academics	Superimposed political messages onto TV broadcasts	Political	[2]
1986	Hijacking	Ground Segment	Home Box Office (HBO) satellite TV network - Galaxy 1 satellite	Commercial	Single insider	Disrupted uplink and displayed messages for 4 to 5 minutes of HBO on US East coast	Warning	[3]
1987	Hijacking	Data Comms	PlayBoy Channel	Commercial	Insider from Christian Broadcasting Network	Signal was hijacked/jammed – character generator and transmitter at CBN matched the tape recording of the jamming	Warning	[1]
1987	Hijacking	Data Comms	Chicago-based TV broadcasts	Commercial	Unknown	Max Headroom impersonator hijacked TV signals for two chicago-based stations.	Unknown	[1]
1995	Jamming	Data Comms	Kurdish satellite TV channel MED-TV	Commercial	Turkey	Transmissions of MED-TV from the Eutelsat satellite were jammed intentionally as it was believed to be a ``mouthpiece" for terrorist groups.	Political	[1]
1997	Jamming	Data Comms	Communication satellite APSTAR-1A	Government	Indonesia	Indonesian satellite transmitted interference to jam APSTAR-1A due to its use of a disputed orbital slot cite	Political	[1,4]
1997	CNE	Ground Segment	NASA	Government	Unknown	Cyber attack on NASA's Goddard Space Flight Centre – able to control computers which designed and tested command and control codes, and then transferred information overseas	State Espionage	[1]
1998	Control	Space Segment	US-German ROSAT satellite	Government	Russia (allegedly)	Satellite turned towards the sun, damaging itself and rendering itself useless. Linked (tenuously) to a intrusion at the Goddard Space Flight Centre. Could have also been a malfunction?	Unknown	[1]
1998	CNE	Ground Segment	Pentagon network	Government/Military	Hacking Group Masters of Downloading	Hacking group claimed to have stolen satellite control software from Pentagon network – Pentagon denies this but revealed that a less secure network containing sensitive information had been breached. Also the group was considering “selling the information to international terrorist groups or foreign governments”	Criminal- selling information on for esp/terrorism	[1]
1998	Denial of Service (Accidental)	Space Segment	PANAMSAT Galaxy 4 sat	Commercial	N/A Accidental	On-board processor anomaly disabled 80-90% of pagers across US for 2-4 days, blocked credit card transactions.	Accident	[1]

2000	Jamming	Data Comms	British and US military tanks	Military	French Security Agency	GPS navigation signals used in British and US military tanks were jammed in tank trial for the Greek army. intended to make US and British tanks look inferior to others so that Grecian military chose other tanks.	State Espionage	[1,5]
2001	CNE	Ground Segment	NASA facilities	Government	British Hacker Gary Mckinnon	Exploited default credentials to gain access to networks at five NASA facilities	Hack and Leak	[6]
2002	Hijacking	Data Comms	Chinese satellite TV broadcasts	Commercial	Falun Gong cult	"Television signals illegally broadcast by the Falun Gong cult cut into transmissions using the Sino Satellite (SINOSAT) from June 23 to 30, blocking the World Cup finals for viewers in some rural and remote areas in China."	Political	[7]
2002	CNE	Ground Segment	Marshall Space Flight Center	Government	China (suspected)	Intruder was able to penetrate into the network and steal design of rocket engines	State Espionage	[1]
2002	Jamming	Data Comms	Accidental- civilian GPS	Civilian	Poorly installed CCTV camera by man from Douglas	Accidental interference from poorly installed CCTV camera blocked GPS signals within a kilometre.	Accident	[8]
2002	Eavesdropping	Data Comms	NATO surveillance	Military	Radio Amateur	Radio Amateur from England was able to eavesdrop on satellite signals from NATO surveillance flights	Research	[9]
2003	Jamming	Data Comms	Telstar 12 satellite TV transmissions	Civilian	Iran and Cuba	US-sponsered news transmissions by the Telstar 12 satellite into Iran were disrupted by a Cuban electronic-intelligence facility	Political	[10]
2004	Hijacking	Data Comms	Chinese satellite TV broadcasts	Commercial	Falun Gong cult	"On Saturday evening, television programmes promoting Falun Gong appeared on the feed beamed into China from a satellite owned by the Hong Kong company AsiaSat."	Political	[11]
2005	Jamming	Data Comms	Satellite radio station ``Sout Libya" uplinks to the Eutelsat HotBird and Telstar 12 satellites	Civilian	Libyan Government	Within minutes of the Sout Libya radio station broadcasting, the Libyan government jammed the radio station's signal with a high-powered one. This jamming also affected many British and European TV and radio station and is alleged to have disrupted American communications as well. Same behaviour observed when Sout Libya changed satellite provider cite.	Political	[12]
2005	CNE	Ground Segment	Kennedy Space Center's Vehicle Assembly Building, NASA satellite control complex in Maryland, Johnson Space Center in Houston	Government	Taiwan (suspected)	Malware gathered data from computers in the VAB, then spread to other networks in Maryland and Houston. 20 GB of compressed data was sent to Taiwan	State Espionage	[1]

2005	Jamming	Data Comms	Telecom satellites	Commercial/Government/Military	Libyan Government	Disrupted signal for several TV and radio stations which served Britain and Europe and American diplomatic, military and FBI comms	Political	[1]
2006	Hijacking	Data Comms	Al Manar TV station	Commercial	Israel (state-sponsored)	Disrupted transmission to broadcast ant-Hezbollah propaganda	Political	[1]
2006	Jamming	Data Comms	Thuraya mobile sat comms	Commercial	Libyan nationals	Signals jammed for six months, in an attempt to disrupt smuggling operations which used the Thuraya sat phones	Stop criminal activity	[1]
2006	Phishing/CNE	Ground Segment	NASA employees	Government	Unknown	NASA officials opened an email and clicked on a link which then infected and compromised workstations at their Washington headquarters. This allowed access to files containing cutting-edge satellite research	State Espionage	[1]
2007	Hijacking	Data Comms	Satellite TV broadcast(Intelsat satellite vacant Ku-band transponder)	Commercial	Liberation Tigers of Tamil Eelam (LTTE)	Illegal broadcast of Tamil Tigers (LTTE) propaganda	Political	[1]
2007	Internet Hijacking	Data Comms	End users of government, military, research and pharmaceutical organizations	Military/Civilian/Government/Commercial	Russsian Turla Hacking group	“exploiting the vulnerability of asynchronous satellite internet connections to sniff traffic, distilling the IP addresses of satellite subscribers. All the attackers need then is to set up their servers with the same IPs, configure these addresses into their malware and, after a successful infection,wait for its call for C&C”	Criminal	[13]
2007	Hijacking	Ground Segment	Czech TV programme	Commercial	Unknown	Camera;s which usually show imagery of Prague and other locations, one had a feed tampered with onsite and video stream was replaced.(Video showed CGI of small nuclear explosion and white noise)	Warning	[1]
2007	Hijacking	Data Comms	WJLA’s digital/HD signals	Commercial	N/A Accidental	Grainy photo interrupted signals for two hours. Originally thought to be signal intrusion, was confirmed to be result of a malfunctioning HDTV encoder	Accident	[1]
2007	CNE	Ground Segment	Goddard Space Flight Center	Government	Unknown	Attack affected networks which processed data from the Earth Observing system	State Espionage	[1]
2007	Jamming	Space Segment	Landsat-7	Government	Unknown	Satellite “experienced 12 or more minutes of interference”	Unknown	[14]

2007	CNE	Space Segment	ISS computers	Government	Compromised laptop brought on by Russian astronaut	Unknown- virus was designed to steal credentials for popular games and send back to central server. SpaceRef:"Virus was never a threat to any of the computers used for cmd and cntl and no adverse effect on ISS Ops." Also brought to light than no AV measures were present and that windows XP was still in use in the systems, which prompted use of Linux.	Accident	[15,16]
2007	ASAT Incident	Space Segment	Chinese weather satellite	Government	China	Anti-satellite test with kinetic kill weapon destroyed defunct chinese weather satellite and created vast amounts of space debris	Satellite destruction	[17,18]
2008	Control	Unknown (but Ground is hypothesised)	Terra EOS AM-1 satellite	Government	Unknown	Satellite experienced several minutes of interference and the capability for the attacker to command was achieved but no commands were given. This occurred twice in 2008, in June, then again in October. Report states that commercially operated ground stations may have been weak point, however KSAT deny this	State Espionage	[1,14]
2008	Control	Unknown (but Ground is hypothesised)	Terra EOS AM-1 satellite	Government	Unknown	Satellite experienced several minutes of interference and the capability for the attacker to command was achieved but no commands were given. This occurred twice in 2008, in June, then again in October.	State Espionage	[1,14]
2008	Control	Space Segment/ Ground Segment	International Space Station	Government	Unknown	A trojan horse infected the Johnson Space Centre's computers which provide an uplink to the ISS to attackers, disrupting several systems on board. This was aided by the out-of-date software in use onboard the ISS	State Espionage	[1]
2008	Jamming	Data Comms	Landsat-7	Government	Unknown	Satellite "experienced 12 or more minutes of interference. The responsible party did not achieve all steps required to command the satellite"	Unknown	[1,14]
2008	ASAT Incident	Space Segment	USA-193 recon satellite	Military	USA	USA-193 satellite failed shortly after launch in 2006. US military confirmed they had shot it down with a missile to destroy it	Satellite destruction	[19]
2009	Hijacking	Data Comms	US Navy communication satellite frequencies	Military	Various- university professors, electricians, truckers and farmers	Hijack of frequencies for personal CB radio use	Personal use	[1]
2009	Eavesdropping	Data Comms	US Military Predator Drones	Military	Iraqi Shi'a militia group	Insurgents captured unencrypted live video feeds from US military unmanned aircraft using a commercial software tool named SkyGrabber	State Espionage	[1]

2010	Denial of Service (Accidental)	Ground Segment	Accidental – GPS receivers	Civilian & Military	GPS software update	software update to gps ground segment caused a denial of service , impacting several thousand receivers	Accident	[8,20]	
2010	Jamming	Data Comms	Persian-language satellite broadcasts	Commercial	Iranian source	Intentional jamming of broadcasts of BBC, Deutsche Welle and Eutelsat	Political	[1]	
2011	Jamming	Data Comms	LuaLua TV (Bahrani current affairs network)	Commercial/Civilian/Governmental	Within Bahrain	Jammed for four hours after first transmission	Political	[1,21]	
2011	Jamming	Data Comms	Thuraya satellites	Commercial	Libyan nationals	Signals jammed for six months, in an attempt to disrupt smuggling operations which used the Thuraya sat phones	Stop criminal activity	[1]	
2011	Jamming	Data Comms	Ethiopian Sat TV (ESAT)	Commercial	Ethiopian & Chinese Governments	Jammed ESAT signals by 2 governments	Political	[1]	
2011	CNE	Ground Segment	JPL	Government	Chinese IPs	Attack on JPL network, compromising credentials of employees, able to modify, add, delete files and users, full control over these networks. Another 46 APT attacks were reported, with 13 successfully compromising agency computers.	State Espionage	[22]	This plus another 13 successful attacks for NASA systems in 2011.
2011	Theft/Loss	Ground Segment	NASA unencrypted laptops	Government	Unknown	Disclosure of algorithms used to command ISS. Another 47 mobile computing devices reported lost or stolen between 2009 and 2011.	State Espionage	[22]	This plus another 47 incidents between 2009 and 2011
2011	CNE	Ground Segment	European Space Agency	Government	Hacker TinKode	Posted screenshots of admin, FTP, network management credentials on internet mailing list	Hack and Leak	[23]	
2012	Jamming	Data Comms	Eritrean state-run sat TV	Government	Ethiopian Government (accused)	Blocked transmissions	Political	[1]	
2012	Denial of Service	Ground Segment	BBC Persia satellite feeds and phone lines	Commercial	Iran (suspected)	“suffered attempts to jam BBC Persian phone lines in London and a "sophisticated cyber-attack" on its systems.”	Political	[24]	
2013	Jamming	Data Comms	GPS receiver in Limo (civilian GPS)	Civilian	American Limo driver	Driver installed an illegal GPS jammer in his car to thwart the tracker in his car. Ended up jamming signals in s GPS-guidance system at Newark Airport	Personal use	[25]	
2013	Jamming	Data Comms	Al-Jazeera Egyptian broadcasts	Government (state-run media outlet)	Unknown, but reported to have originated from outside Cairo	Jamming of Al-Jezeera egyptian TV signals	Political	[26]	
2013	Spoofing	Data Comms	GPS navigtaion system in a yacht	Civilian	Researchers	“ "proof-of-concept" attack was successfully performed in June, 2013, when the luxury yacht White Rose of Drachs was misdirected with spoofed GPS signals...which altered the course of the yacht”.	Research	[27]	

2014	Jamming	Data Comms	ARABSAT TV downlinks	Commercial	Ethiopian Source	Jammed signals which disturbed many TV channels- Arabsat speculated that it may be accidental and jammers were targeting nearby satellites as Arabsat doesn’t broadcast in Ethopia or Eritrea.	Political	[28]
2014	CNE	Ground Segment	Germany’s space research centre in Cologne	Government	Unknown but state-level cyber actors	Suffered an intrusion, “malware on machines used by researchers and sysadmins”	State Espionage	[29]
2014	CNE	Ground Segment	National Oceanic and Atmospheric Administration	Government	China (suspected)	Four websites were hacked, government was forced to shut down services, however purpose/impact of the attack was not made public	State Espionage	[30,31]
2014	Hijacking	Data Comms	Isreali Channel 10 broadcasts	Commercial	Al-Qassam Brigades (Hamas)	Took over satellite feed to broadcast propaganda	Political	[32]
2015	Eavesdropping	Data Comms	Iridium communications constellation	Commercial	Security Researchers	Iridium satellite constellation communications were analysed and decoded to reveal clear text pager information	Research	[33]
2015	CNE	Ground Segment	ESA website and users	Government	Hacking group Anonymous	Published database schema of ESA website, with info relating to users, collaboraters and subscribers	Hack and Leak	[34]
2015	CNE	Ground Segment	NASA	Government	Hacking collective Anonsec	Anonsec “bought access to an agency computer from another hacker.” and then used it to pivot into network. Published 250 GB dump of data.	Hack and Leak	[35]
2016	Phishing/CNE	Ground Segment	Aerospace companies	Commercial/Government	APT28 hacking group (sponsored by Russian intelligence	attackers used “a phishing email to lure the user into downloading a file that looks like a PDF but instead is malicious executable code”. Contained trojan.	State Espionage & Corporate Espionage	[36,37]
2016	Hijacking	Data Comms	Israeli Channel 2 broadcast	Commercial	Hamas	broadcast was “suddenly interrupted, and TV screens filled instead with images and messages of incitement from Hamas, which warned of fresh terror attacks.”	Political	[38]
2017	Spoofing	Data Comms	Ships in Black Sea	Civilian	Russia (allegedly)	Maritime navigation systems onboard several vessels reported incorrect ship locations from false GPS signals. ““trying to trigger UAV geo-fencing, which prevents UAVs from flying near airports”	Geo-fencing	[39]
2017	Jamming	Data Comms	Accidental- civilian GPS	Civilian	GPS jammer in parked car	Driver in France left an operational GPS jammer in his car which was parked at Nantes airport – interfered with aircraft tracking systems	Personal use	[40]
2017	CNE/Phishing	Ground Segment	Aerospace companies	Commercial/Military	APT33 group (iran)	Phishing emails sent into aerospace companies to download trojan backdoor.	State Espionage & Corporate Espionage	[41]
2017	Hijacking	Data Comms	Libyan Television broadcats	Commercial	Gaddafists	Broadcasts were interrupted by Gaddafists	Political	[42]
2017	Spoofing	Data Comms	GPS time spoofing for TOTP authentication method	Civilian	Researchers	Able to spoof GPS timing in an air-gapped network to bypass TOTP authentication	Research	[43]

2018	CNE	Ground Segment	Satellite Operator	Commercial	Computers in China, Thrip group	“looking for and infecting computers running software that monitors and controls satellites” to potentially disrupt satellite operations	Corporate Espionage	[44]
2018	CNE	Ground Segment	NASA	Government	Unknown	“According to an internal memo circulated among staff on Tuesday, in mid-October the US space agency investigated whether or not two of its machines holding employee records had been compromised, and discovered one of them may have been infiltrated by miscreants. It was further feared that this sensitive personal data had been siphoned from the hijacked server.”	State Espionage	[45,46]
2019	ASAT Incident	Space Segment	Microsat-R military satellite	Military	India	Microsat-R test satellite was destroyed in LEO by ASAT weapon	Satellite destruction	[47]

Electronic Supplementary Material

References

Author

1 Fritz, J.: Satellite Hacking: A Guide for the Perplexed. In: Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, December 2012-May 2013, pp21-50

2 Hanasz, J.: Telewizja ,,Solidarność" Toruń 1985 r. Url:https://web.archive.org/web/20091206064447/http://w.icm.edu.pl/tvS/tvs.htm (archive) Accessed: 08/07/2019

3 SiGNaLToNoiSe.Net: The Story of Captain Midnight. Url: https://web.archive.org/web/20070128101239/http://www.signaltonoise.net/library/captmidn.htm (archive) Accessed 08/07/2019

4 United States General Accounting Office: Critical Infrastructure Protection Commercial Satellite Security Should Be More Fully Addressed. In: Report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate. 2002

5 Lt. Col. Adams, T. K.: 10 GPS Vulnerabilities Url: http://www.c4i.org/gps-adams.html Accessed 08/07/2019

6 Telegraph.co.uk: Gary McKinnon profile: Autistic 'hacker' who started writing computer programs at 14 Url: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/4320901/Gary-McKinnon-profile-Autistic-hacker-who-started-writing-computer-programs-at-14.html Accessed 08/07/2019

7 Embassy of the People’s Republic of China in the United States of America: Chinese satellite TV hijacked by Falun Gong cult (07/08/02) Url: http://www.china-embassy.org/eng/zt/ppflg/t36611.htm Accessed 08/07/2019

8 The Royal Academy of Engineering: Global NavigationSpace Systems:reliance and vulnerabilities Url: https://www.raeng.org.uk/publications/reports/global-navigation-space-systems. March 2011 Accessed 08/07/2019

9 Urban, M.: Enthusiast watches Nato spy pictures Url: http://news.bbc.co.uk/1/hi/programmes/newsnight/2041754.stm June 2002 Accessed 08/07/2019

10 Waller J. M.: Iran and Cuba Zap U.S. Satellites In: Insight Magazine Url: http://jmichaelwaller.com/wp-content/uploads/2016/08/IM-Telstar-Aug2003.pdf August 2003 Accessed 08/07/2019

11 Hogg, C.:HK probes Falun Gong 'hacking' Url:http://news.bbc.co.uk/1/hi/world/asia-pacific/4034209.stm November 2004 Accessed 08/07/2019

12 BBC News: Libya jamming 'exposed vulnerability' Url: http://news.bbc.co.uk/1/hi/sci/tech/4602674.stm January 2006 Accessed 08/07/2019

13 Kaspersky: Turla Hiding in the Sky Threat Announcement Url: https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf Accessed 08/07/2019

14 2011 Report to Congress of the U.S.-CHINA Economic and Security Review Url: https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf Accessed 08/07/2019

15 BBC News: Computer viruses make it to orbit Url: http://news.bbc.co.uk/1/hi/technology/7583805.stm August 2008 Accessed 08/07/2019

16 Cowing, K.: NASA Discovers Computer Virus Aboard the International Space Station Url: http://www.spaceref.com/news/viewnews.html?id=1305 Accessed 08/07/2019

17 Nicholson, B.: World fury at satellite destruction Url: https://www.theage.com.au/national/world-fury-at-satellite-destruction-20070120-ge416d.html Accessed 08/07/2019

18 Center for Space Policy and Strategy: Space Traffic Management in the Age of New Space Url: https://aerospace.org/sites/default/files/2018-05/SpaceTrafficMgmt_0.pdf Accessed 08/07/2019

19 News24.com: US shoots down rogue satellite Url: https://web.archive.org/web/20080222154922/http://www.news24.com/News24/World/News/0,,2-10-1462_2274693,00.html (archive) Feb 2008 Accessed 08/07/2019

20 Ferrazzani, M. and Zilioli, I.: ESA facing Cyber Security Concerns In: EUSpace Jean Monnet Module 2018 Url: http://www.eu-space.eu/images/2018/document/Slides/Slides-Ferrazzani-Zilioli.pdf Accessed 08/07/2019

21 Atkinson, S.:Bahrain TV station struggles as signal blocked Url: https://www.bbc.co.uk/news/business-15699332 November 2011 Accessed 08/07/2019

22 Martin, P. K.:NASA Cybersecurity: An Examination of the Agency’s Information Security In: Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology February 2012 Url:https://oig.nasa.gov/docs/FINAL_written_statement_for_%20

23 Leyden, J.: Royal Navy hacker claims to have broken into space agency site Url: https://www.theregister.co.uk/2011/04/18/esa_website_hack/ Accessed 08/07/2019

24 Halliday, J.: BBC fears Iranian cyber-attack over its Persian TV service Url: https://www.theguardian.com/media/2012/mar/14/bbc-fears-iran-cyber-attack-persian March 2012 Accessed 09/07/2019

25 CBE New York: N.J. Man In A Jam, After Illegal GPS Device Interferes With Newark Liberty Operations Url: https://newyork.cbslocal.com/2013/08/09/n-j-man-in-a-jam-after-illegal-gps-device-interferes-with-newark-liberty-operations/ August 2013 Accessed 09/07/2019

26 O’Carroll, L.: Al-Jazeera: jamming traced to sites near Egyptian military bases Url: https://www.theguardian.com/media/2013/sep/03/al-jazeera-jamming-traced-egyptian-military September 2013 Accessed 09/07/2019

27 The University of Texas at Austin: UT Austin Researchers Spoof Superyacht at Sea Url: http://www.engr.utexas.edu/news/archive/7649-superyacht-gps-spoofing July 2013 Accessed 09/07/2019

28 Arabsat.com: Arabsat is subject to Jamming and its Engineers succeed in locating its source Url: https://www.arabsat.com/NewsDetails.aspx?pageid=428&lang=2 May 2014 Accessed 09/07/2019

29 Muncaster, P.:German space centre endures cyber attack Url: https://www.theregister.co.uk/2014/04/15/dlr_attacked_china_apt_trojans/ April 2014 Accessed 09/07/2019

30 Pagliery, J.: U.S. weather system hacked, affecting satellites Url: https://money.cnn.com/2014/11/12/technology/security/weather-system-hacked/index.html December 2014 Accessed 09/07/2019

31 Flaherty, M.P. and Samenow, J. and Rein, L.: Chinese hack U.S. weather systems, satellite network Url: https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html?utm_term=.19171e40af67 Novembe

32 Leyden, J.: Hamas hacks Israeli TV sat channel to broadcast pics of Gaza wounded Url: https://www.theregister.co.uk/2014/07/15/hamas_hack_israeli_sat_tv/ July 2014 Accessed 09/07/2019

33 Sec and schneider:Iridium Hacking: please don't sue us In:Chaos Communication Camp 2015

34 Storm, D.:Attackers hack European Space Agency, leak thousands of credentials 'for the lulz' Url: https://www.computerworld.com/article/3014539/attackers-hack-european-space-agency-leak-thousands-of-credentials-for-the-lulz.html December 2014 Accessed 09/07/2019

35 Thomson, I.:Hackers mirror 250GB of NASA files on the web Url: https://www.theregister.co.uk/2016/02/01/250gb_nasa_data_hacked/ February 2016 Accessed 09/07/2019

36 Cyber Defence Magazine: Fancy Bear Hackers use a new Mac Trojan against aerospace industry Url: https://www.cyberdefensemagazine.com/fancy-bear-hackers-use-a-new-mac-trojan-against-aerospace-industry/ September 2016 Accessed 09/07/2019

37 Jackson Higgins, A.:Russian 'Fancy Bear' Hackers Hit Mac OS X With New Trojan Url:https://www.darkreading.com/operations/russian-fancy-bear-hackers-hit-mac-os-x-with-new-trojan/d/d-id/1327016 September 2016 Accessed 09/07/2019

38 The Times of Israel: Hamas hacks into Israeli TV and threatens: ‘Terror will never end’ Url: https://www.timesofisrael.com/hamas-hacks-israeli-tv-the-terror-will-never-end/ March 2016 Accessed 09/07/2019

39 Leid, H.:GPS freaking out? Maybe you’re too close to Putin Url:https://web.archive.org/web/20170925202637/https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/ September 2017 Accessed 09/07/2019

40 Resilient Navigation and Timing Foundation: GPS Jammer Delays Flights in France Url: https://rntfnd.org/2017/09/15/gps-jammer-delays-flights-in-france/ September 2017 Accessed 09/07/2019

41 O’Leary,J. and Kimble, J. and Vanderlee, K. and Fraser, N.:Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware Url: https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html Septen

42 The American Gaddafist: Gaddafists Hack Libyan TV Signal March 5, 2017: https://www.youtube.com/watch?v=QwjAZGoGjPo&app=desktop Accessed 09/07/2019

43 Robinson, D.: Using GPS Spoofing to control time In: DEFCON 25 July 2017 Url: https://www.youtube.com/watch?v=isiuTNh5P34 Accessed 09/07/2019

44 Symantec.com: Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies Url: https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets June 2018 Accessed 09/07/2019

45 Williams, C: Houston, we've had a problem: NASA fears internal server hacked, staff personal info swiped by miscreants Url: https://www.theregister.co.uk/2018/12/18/nasa_server_hack/ December 2018 Accessed 09/07/2019

46 spaceref.com: Potential Personally Identifiable Information (PII) Compromise of NASA Servers Url: http://spaceref.com/news/viewsr.html?pid=52074 December 2018 Accessed 09/07/2019

47 Anantha Krishnan M:Explained Mission Shakti Url:https://english.manoramaonline.com/news/nation/2019/03/27/mission-shakti-drdo-asat-missile-hit-microsat-r-isro.html March 2019 Accessed 08/07/2019

IT_%20hearing_February_26_edit_v2.pdf Accessed 08/07/2019

er 2014 Accessed 09/07/2019

nber 2017 Accessed 09/07/2019