



NITETeAM 

INTELLIGENCE CODEX V1.0



History & Background	8
The Black Watchmen	8
NITE Team 4 Unit	8
STINGER Terminal	8
Off-Net Intrusion Group (ONIGRU)	9
Social Engineering Team (SET) 6 Unit	9
SECTION 8	9
Main Characters	10
Agent Catherine Wheeler	10
Agent Dylan Voorhees	10
Artificial Intelligence F.A.Y	10
Artificial Intelligence Softcrash	11
Agent Patricia C. Conway	11
Agent Samantha Morris	11
Raindoll	11
Dr. Ripper	12
Organization	13
4Sight	13
Cronix Security Solutions	13
Deft Security	13
Dreadnot	13
Dwellers	14
Eastern Light	14
Forgotten Shadows	14
ICM32	14
Magi	15
Lilin	15
Mentor	15
Morpho Medical	15
Noblesse Oblige	16
Null & Void	16
Orion's Watch	16
PCBL	16
PCI	16
Rhopagroup	17



Sigil	17
Teulai Seuta	17
The Arbiters of Alexandria	18
The Harbingers	18
The Internet Creepers	18
The Order of Morpheus	18
Vault Advisors	19
Vestige	19
Rising Sun	19
Reality Deviant	19
Intelligence Cycle	21
Core Concept (traditional)	21
Direction	21
Collection	21
Processing	22
Analysis	22
Dissemination	22
Feedback	22
Intelligence Cycle (target-centric approach)	23
Models in intelligence	23
Sources of intelligence information	23
Populating the model	24
Applications of the target-centric approach to intelligence	24
Intelligence Collection	25
HUMINT	25
Cyber-HUMINT	26
GEOINT	26
MASINT	26
OSINT	27
SIGINT	28
TECHINT	29
CYBINT/DNINT	29
FININT	30
Intelligence Analysis	31
Overview	31
Computer Network Operations (CNA/CNE/CND)	32
CNO in the military domain	32



Types of Military CNO	32
Cyberspace Operations	33
Counterintelligence	33
Categories of counterintelligence	33
OPSEC	34
Relationship with Intelligence Agencies	35
Australian Signals Directorate (ASD)	35
Australian Secret Intelligence Service (ASIS)	35
Canadian Communications Security Establishment (CSE)	36
Canadian Security Intelligence Service (CSIS)	36
China Ministry of State Security (MSS)	37
PLA Unit 61398	37
GhostNet	38
France Direction Générale De La Sécurité Extérieure (DGSE)	38
German Bundesnachrichtendienst (BND)	39
India Research and Analysis Wing (RAW)	39
Iran Ministry of Intelligence (VAJA)	39
Israel Institute for Intelligence and Special Operations (MOSSAD)	39
Japan Cabinet Intelligence and Research Office (Naichō)	40
New Zealand Government Communications Security Bureau (GCSB)	40
North Korea Bureau 121 (B121)	41
Malware Development & Attacks	41
Pakistan Inter-Services Intelligence (ISI)	42
Russian Federal Security Service (FSB)	42
COZY BEAR aka CozyDuke	43
FANCY BEAR aka Sofacy	44
Russian Foreign Intelligence Service (SVR)	44
Russian Main Intelligence Agency (GRU)	45
South African State Security Agency (SSA)	46
South Korea National Intelligence Service (NIS)	46
United Kingdom Government Communications Headquarters (GCHQ)	46
Joint Threat Intelligence Research Group (JTRIG)	47
Major GCHQ Projects & Programs	48
Additional GCHQ sources	48
United States Army Intelligence Support Activity (USAISA)	49
Pathfinder Missions	49
Current Status	49



United States Central Intelligence Agency (CIA)	50
United States Director of National Intelligence (DNI)	50
United States National Geospatial-Intelligence Agency (NGA)	50
United States National Security Agency (NSA)	50
Special Source Operations (SSO) - Domestic Collection	51
Global Access Operations (GAO) - Overseas Collection	51
Tailored Access Operations (TAO) - Hacking Operations	51
United States Special Activities Division (SAD)	52
Tools & Technology	54
DNS & Vhost Mapping	54
Fingerprint	54
Hydra Terminal	54
Password Attack	55
Social Engineering Toolkit	55
Man in the Middle	56
Turbine C2 registry	56
QUANTUM Exploit Suite	56
Tasking with QUANTUM	57
FOXACID Exploit Servers	58
QUANTUM Plugins	60
FashionCleft	61
Warrior Pride CID Backdoor	62
XKeyscore	62
Summary	63
Data Sources	64
Capabilities	65
Kali Linux	66
Metasploit Project	67
MITRE ATT&CK framework	68
Common Vulnerabilities and Exposures Registry	68
Special Tactic, Tradecraft and Methods	69
Drone Feed Hacking - ANARCHIST	69
VSAT Monitoring - GHOSTHUNTER	70
Technical Functionality	71
Tasking Process	71
Target Travel Analytics - CO-TRAVELER	72
FASTFOLLOWER	73



Active/Passive Exfiltration (APEX) - TURBULENCE	74
Darknet Operation	75
Honeypot	75
Famous Hacks	76
The Morris Worm	76
Phonemasters	76
Citibank / Valdimir Levin	76
Melissa Virus	76
Mafiaboy	76
Delta Airlines / Sven Jaschan	77
Operation Get Rich	77
Iceman	77
Conficker	77
Epsilon	78
Playstation Network	78
Comodo	78
Citigroup	78
Saudi Aramco	79
Spamhaus	79
Global Bank Spear Phishing	79
Recent Hacks	81
Tumblr Hack (2013)	81
MT.Gox Bankruptcy (FEB.2014)	81
White House Intrusion (OCTOBER.2014)	81
Sony Picture Breach (NOVEMBER.2014)	81
Globe Telecom Hack (NOVEMBER.2014)	81
United States Office Public Records Stolen (JUNE 2015)	81
Ashley Madison Site Breach (JULY 2015)	82
Bangladesh Bank Robbery (FEB.2016)	82
Wikileaks (JULY.2016)	82
Vietnam Airline Attack (JULY.2016)	82
ISIL Hacker (SEP.2016)	82
DYN Cyber Attack (OCT.2016)	82
Cloudbleed Bug (FEB.2017)	83
The Dark Overlord (APRIL.2017)	83
Wannacry Ransomware (MAY.2017)	83
Cyber Blackmail (MAY.2017)	83



PETYA (JUNE.2017)	83
The Equifax Breach (JULY.2017)	83
Deloitte Breach (SEP.2017)	84
Notorious Hackers	85
Adrian Lamo	85
Albert Gonzalez	85
Anonymous	85
Astra	85
David L. Smith	85
The Dark Overlord	85
Evgeniy Mikhailovich Bogachev	86
Gary Mckinnon	86
James Kosta	86
Jeanson James Ancheta	86
John McAfee	86
Jonathan James	86
Kevin Mitnick	87
Kevin Poulsen	87
Lizard Squad	87
Loyd Blankenship	87
Lulzsec	87
Matthew Bevan	87
Max Ray Butler	88
Michael Calce	88
Morpho	88
Owen Thor Walker	88
Robert Tappan Morris	88
Stephen Wozniak	88
Sven Jaschan	88
The Master of Deception	89
The Syrian Electronic Army	89
The Shadow Brokers	89
Vladimir Levin	89
Glossary & Code Words	90

