

Index

- activist, 7, 15
- actor, 1, 3, 9, 11, 13, 37, 97, 118, 119–21
- Adobe Flash, 69, 89
- Amazon, 47, 65
- Android, 58, 59, 65, 89, 90
- anonymity, 7, 15, 18, 19, 26, 29, 32, 37, 119, 120
- Anonymous, 7, 14–16, 19, 29, 119, 120
- antivirus, 4, 6, 65
- approximation algorithm, 83, 85, 88
- approximation bound, 75, 81, 83
- Artificial Intelligence, 2, 3, 118, 119
- attack, 4–7, 10, 16, 17, 27, 30, 69, 70–6, 79, 80, 82, 84, 85, 88, 90, 93, 101, 105, 106, 116
 - cyber, 1, 14, 37, 38, 54, 67, 95, 96, 98, 118, 120, 121
- attribution, 8, 121
- authentication, 99, 114
- axiom, 72, 73, 76, 78–80, 83, 100
- bag of words, 45, 46, 52, 53, 63
- banking trojan, 1, 2
- banned, 34, 35, 36
- best response, 73, 82, 90, 92, 93
- Bitcoin, 7, 50, 54, 56, 58, 65, 70, 90
- black hat, 13, 14, 16, 17, 32, 36
- black list, 35, 36
- botnet, 1, 6, 47, 50, 65, 69
- branching factor, 107, 114–16
- breach, 2, 10, 13, 27
- browser, 13, 15, 19, 30, 65
- buyer, 1, 34, 35, 67
- capability, 8, 10, 13, 37, 97, 99, 100–7, 110–12, 114, 116, 117
- captcha, 6, 17, 19, 21, 40
- carding, 21, 28, 65
- censorship, 15, 32
- centroid, 62–4
- character ngram, 46, 47, 48, 50, 62, 63
- child pornography, 20, 29
- classification, 31, 42, 43–6, 48–53, 63
- Cleartnet, 14–17, 21, 22, 23, 26, 27, 36, 38, 40, 54
- clustering, 3, 34, 56, 62, 63, 65, 66
- code execution, 2, 59, 99
- computational complexity, 75, 77, 79, 81, 105
- computer, 1, 9, 15, 16, 19, 37, 70, 74, 90, 96, 97, 119
- computer network, 16, 74, 97
- constraint set, 70–3, 76, 77, 78, 80, 81, 85–7, 90
- control system, 3, 96–8, 100, 102, 104, 106, 108, 110, 112, 114, 116
- cosine similarity, 62–4
- cost-benefit, 84, 85, 90, 91, 93, 95
- cracker, 16, 95
- cracking, 14, 16, 65
- credit card, 1, 2, 27, 65
- crime forum, 26, 37
- critical infrastructure, 8, 54, 95, 97, 98, 116
- cross validation, 47, 49, 51
- crypto network, 13, 15, 17
- CVE, 2, 42, 60, 61, 62, 69, 95, 99, 112, 114
- cyber adversary, 11, 96, 98
- cyber attack, 1, 14, 37, 38, 54, 67, 95, 96, 98, 118, 120, 121
- cyber attacker, 11, 96
- cyber capability, 13, 37
- cyber defender, 1, 9, 38, 69

- cyber defense, 56, 118, 120, 121
- cyber domain, 14, 37
- cyber intelligence, 2, 38, 40, 42, 44, 46, 48, 50, 52, 54
- cyber threat, 1–4, 6, 8–13, 30, 37–40, 45, 54, 56, 66, 67, 95, 97, 117–21
 - intelligence, 1–13, 37–40, 54–6, 66–8, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 95, 117, 118, 121
- Darknet forum, 19–21, 32, 33, 49, 54, 119
- Darknet market, 1–3, 21, 36, 43, 45, 51, 53, 56, 57, 60, 66, 67, 69, 70, 89, 90, 104, 117, 119, 120
- darknetizens, 26, 29, 32
- Darkode, 10, 26
- Darkweb, 6, 7, 9, 10, 13–24, 26–30, 32–4, 36–8, 40, 42, 44, 46, 48, 50, 52, 54, 57, 69, 96, 97, 117
- data breach, 2, 27
- data driven, 7, 67, 68, 120
- database, 23, 38, 39, 40, 61, 90
- Distributed Denial of Service (DDoS), 6, 7, 9, 17, 30, 61, 98, 99
- Deepnet, 26, 39, 49, 51, 53, 55, 56
- Deepweb, 6, 7, 9, 15, 117
- deterministic, 73, 74, 76, 78, 82, 87, 88, 93
- depth-first search (DFS), 107–10, 114–16
- digital currency, 30, 34
- Double Oracle, 87–9, 93, 94
- drugs, 23, 29, 42, 45, 54, 69
- Dyre Banking Trojan, 1, 2
- eBay, 35, 65
- email address, 20, 27
- enterprise, 4, 8, 10
- entropy, 62–5
- expected payoff, 72, 78, 79, 82, 93, 94
- exploit analysis, 68, 95
- exploit cost, 95, 105, 106, 112
- Exploit Function, 70, 71, 95
- exploit kit, 1, 26, 27, 37, 61, 62, 65, 67, 117
- exploit market, 1, 36, 38, 45, 51, 54, 58, 68, 69, 70
- exploit price, 59, 112
- exploited vulnerability, 2, 72, 93, 99, 101
- Facebook, 30, 63, 65, 66, 89
- feature extraction, 46, 62, 63
- feature space, 46, 48, 52
- financial fraud, 16, 21
- fingerprinting, 19, 32
- fixed point, 103, 104, 106
- focused crawler, 54, 55
- forum administrator, 19, 23, 27, 34, 36
- forum board, 17, 20, 29
- forum thread, 42, 43, 49, 50, 52
- Freenet, 6, 15
- FTP, 35, 90
- Fully Undetectable (FUD), 6, 69, 89
- gain access, 17, 27, 28, 71, 99
- game theory, 67, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90
- government, 1, 5, 8, 10, 11, 14, 32, 67
- graph, 44, 57, 69
- greedy algorithm, 84, 85, 90
- Hacking as a Service (HaaS), 30, 31
- hack, 8, 24, 46, 95
- hacker, 1–6, 10, 12–18, 20–30, 38, 40, 43, 45, 46, 51, 55–8, 95, 118–21
 - malicious, 4–7, 9, 13, 14, 16–18, 20, 22–6, 28–30, 32, 34, 36, 56, 58, 66, 69, 70, 118, 119
- hacking community, 6, 7, 37, 120
- hacking tool, 47, 63, 65, 89
- Hacktivism, 7, 119
- Hacktivist, 8, 10, 16, 37, 119
- hardware, 10, 89, 97
- heuristic, 96, 107, 110–14
- Hitting Set, 77–84, 86, 87
- homeland security, 8, 69
- Honeypot, 8, 69
- HTML, 2, 15, 40, 41, 52–4
- HTTP Request, 99, 100, 102
- I2P, 1, 6, 15, 19
- industrial control (IC) infrastructure, 3, 96
- industrial control (IC) network, 98, 99
- industrial control system (ICS), 3, 96–8, 100, 102, 104, 106, 108, 110, 112, 114, 116, 121
- infrastructure, 3, 6, 8, 38, 54, 67, 68, 95–8, 116
- intelligence analysis, 37, 55
- interdisciplinary, 3, 118
- Internet, 1, 6, 10, 13, 15, 16, 19, 21, 25, 26, 32, 34, 39, 54, 59, 69, 97, 118
- intrusion detection, 4, 69
- keyloggers, 47, 65, 66

- Latent Dirichlet Allocation (LDA), 45, 53
- lattice, 96, 99
- law enforcement, 5, 8, 10, 14, 24, 25, 27, 30, 32, 54, 69, 119
- leet, 16, 34
- Linux, 6, 19, 65, 69, 89–92, 94, 99, 100
- machine learning, 2, 3, 37–9, 42, 43, 51, 55, 62, 118, 121
- malicious hacker, 4–7, 9, 13, 14, 16–18, 20, 22–6, 28–30, 32, 34, 36, 56, 58, 66, 69, 70, 118, 119
- malware, 1, 2, 5–9, 14, 21, 24, 26–8, 30, 35, 37, 38, 40, 66, 96–8, 118, 120, 121
- Microsoft Windows, 1, 89
- Minimax, 74, 75, 77, 81, 82, 87, 89
- Naive Bayes, 43, 51
- nation state, 4, 8, 10
- National Institute of Science and Technology (NIST), 61, 112, 114, 116
- National Vulnerability Database (NVD), 61, 112, 114, 116
- Olbanian, 26, 34
- optimal strategy, 68, 96, 105
- optimization, 73, 81, 82, 84, 105
- Padonkaffsky Jargon, 26, 34
- penetration tester, 67, 68
- Pretty Good Privacy (PGP), 19, 25–7, 65
- phishing, 6, 65, 66
- Point of Sale (PoS), 2, 27, 65, 89, 90
- pornography, 20, 29, 45
- Power Law, 57, 58
- precision and recall, 47–52
- privilege escalation, 99, 100, 114
- product vendor, 36, 56, 58, 60, 62, 63, 66
- programmer, 15, 27
- programming, 16, 29, 121
- proxy, 35, 120
- Rand Index, 62, 64
- Remote Access Trojan (RAT), 14, 50, 65
- Remote Code Execution (RCE), 2, 59, 89, 99
- reputation, 7, 19, 20, 24–6, 31, 42, 57
- reverse engineer, 93, 95
- Russian forum, 2, 21, 26, 27, 30, 31, 34, 35, 49–51
- Russian hacker, 2, 21, 26, 27
- script kiddy, 16, 27, 28
- security analyst, 38, 40, 43, 44, 47, 50, 53
- security game, 3, 67–71
- semi-supervised learning, 43, 44, 48–51
- Set Cover, 81, 84–7, 93, 105, 106
- Shellshock Vulnerability, 99–102
- social network, 57, 59, 66
- SQL Injection, 35, 47
- Stuxnet, 13, 97, 98
- submodularity, 72, 79, 80, 83, 84
- subreddit, 36, 39, 41, 42, 51, 52
- supervised learning, 43, 44, 48–51, 66
- surveillance, 14, 32
- Support Vector Machine (SVM), 43, 48–53
- terrorism, 8, 17, 69
- threat actor, 3, 9, 11, 97, 118–21
- threat intelligence *see* cyber threat: intelligence
- TOR (The Onion Router), 1, 6, 7, 10, 13–15, 17–19, 21, 23, 25, 26, 30, 40, 54
- Trojan, 1, 2, 14
- unsupervised learning, 3, 45, 55, 56, 66, 121
- vendor, 6, 7, 23, 25, 29, 36, 38, 39, 56–63, 65, 66, 120
- vulnerability, 1, 2, 6, 30, 37, 56–8, 60–2, 67, 70–2, 74, 75, 79, 80, 82, 85–7, 93, 95, 96, 97–102, 105, 112, 117
- word ngram, 46, 63
- word stemming, 46, 53
- Wordpress, 69, 89, 95
- Zero Day Exploit (0day), 1, 5, 6, 56–60, 67–9, 89, 97, 98, 117