Stress Tested: The COVID-19 Pandemic and Canadian National Security

http://hdl.handle.net/1880/114134
book

https://creativecommons.org/licenses/by-nc-nd/4.0
Downloaded from PRISM: https://prism.ucalgary.ca
data disparities for COVID-19 and racial and ethnic minorities, 254–55; Global Health Security Agenda (GHSA) and, 100–101; health-care access disparities, 251; intelligence in, 90, 96; migrant and refugee communities, 247, 247–48; pandemic recommendations, 99–101; remittances from, 249; security threats, 91. See also Canada's intelligence and national security community and COVID-19 pandemic

Canada Border Services Agency (CBSA), 231–42; introduction and conclusion, 6, 232, 265–66; 2022 deportation target, 242n4; administrative removals, 238–39; COVID-19 impacts on, 117, 234–35; deportation process and, 233, 234; deportations and removal orders during pandemic, 234, 235–40, 236; Five Eyes and, 236; fraudulent PPE and, 114; immigration detention and COVID-19, 237–38, 239; open-source intelligence, 118; point-of-entry removals, 235–36; recommendations on resuming deportations post-pandemic, 240–42; roles and responsibilities, 233–34; serious, inadmissibility removals, 236, 242n1; voluntary removals, 236–38. See also national security operations

Canada [Minister of Employment and Immigration] v Chiarelli [1992], 233
Canada Border Services Agency; Canadian Armed Forces; Communications Security Establishment; conspiracy theories; criminal justice system; critical infrastructure, and cyber attacks; cyberspace, and malicious non-state actors; Defence Intelligence Enterprise; deportation; Global Public Health Intelligence Network; health intelligence; migrant and refugee communities; national security operations; supply chains; surveillance apparatus and data collection
Canadian Armed Forces (CAF), 145–55; introduction and conclusion, 5, 145, 154–55, 161, 266; adaptations for COVID-19, 147, 161, 164–67; air force, 150–51; counter-pandemic contingency plan (Operation LASER), 146, 163–64, 173, 262; COVID-19 contagion within, 147–48; CSE’s SIGINT operations, 146–47, 148–49, 155, 156n15, 270; expeditionary operations, 149–54, 165–66; land forces, 151–54; maritime operations, 149–50; readiness, 148; recommendations, 10, 155, 270; training delays, 171–72. See also Defence Intelligence Enterprise
Canadian Centre for Cyber Security: accelerated change at, 121; on critical infrastructure risks, 74–75; cybersecurity operations, 129–32; on cyber threat actors, 42; establishment, 128; IT services at, 113; new partners and clients, 116, 267; support for Shared Services Canada, 266; Traffic Light Protocol, 118–19, 122; workplace protection, 136–37. See also national security operations
Canadian Charter of Rights and Freedoms, 196, 197–98, 203, 206, 207
Canadian Forces Information Operations Group, 134, 135–36
Canadian Forces Intelligence Command (CFINTCOM), 167–73; introduction and conclusion, 162, 163, 173; adaptations during COVID-19 lockdown, 169; Canadian Forces Intelligence Group, 170–71, 172–73; command issues, 171; co-operation with intelligence allies, 170, 271; medical intelligence, 168–69; organization of, 168, 168; return to normal, 172–73; role and responsibilities, 167; training delays, 171–72; workplace protection issues, 169–70
Canadian Forces Intelligence Group, 170–71, 172–73
Canadian Forces Joint Imagery Centre, 170, 172
Canadian Forces National Counter-Intelligence Unit, 170, 172
Canadian Forces School of Military Intelligence (CFSMI), 171–72
Canadian Rangers, 147
Canadian Security Intelligence Service (CSIS): Academic Outreach and Stakeholder Engagement branch, 117, 118, 121, 267; authorities to collect information, 126n2, 198–99, 207; business continuity, 110; on COVID-19 online disinformation, 140; CSE’s SIGINT operations, 133; cybersecurity and, 42, 130; GPHIN and, 187; health intelligence and, 96; intelligence from, 90; IT services, 113; managing stress and anxieties, 112; new partners and clients, 269; new products, 117; openness and public outreach, 121; open-source intelligence, 118; staffing, 110; workplace protection, 136. See also national security operations
Canadian Security Intelligence Service Act (CSIS Act), 197, 198–99, 206, 207
Carignan, Jennie, 152
Centers for Disease Control and Prevention (CDC), 252–53
Centre for International Governance Innovation (CIGI), 121
certification, manufacturing, 54, 56
Charter. See Canadian Charter of Rights and Freedoms
Chayer, Marie-Hélène, 164–65
Chiarelli, Canada [Minister of Employment and Immigration] v [1992], 233
China, 54–55, 56, 76–77, 92–93, 98, 195
Choi, Kate, 254
climate change, 64, 92, 93
Collins, Ben, 28n1
Collins, R v [1987], 203
command, military, 171
Communications Security Establishment Act (CSE Act), 128, 130, 140, 207
communications, 127–41; introduction and conclusion, 4–5, 127–28, 139–40, 266; accelerated change in, 121; active and defensive cyber operations, 132; assistance mandate, 9, 130–31, 207; authorities to collect information, 200; cybersecurity operations, 129–32; future considerations, 140–41; GeekWeek conference, 138; new partners and clients, 115–16, 269; openness and public outreach, 121; open-source intelligence, 119; roles and responsibilities, 127; SIGINT operations, 132–35; workplace protection, 135–39. See also Canadian Centre for Cyber Security; national security operations
Communications Security Establishment Act (CSE Act), 128, 130, 140, 207
computer network attack, 132
conspiracy theories, 15–28; introduction and conclusion, 3, 15–16, 28, 263; characteristics of, 18; COVID-19 and, 17–19, 20–21; history of, 17; national security threats and, 25–27; problem of evil and, 18; proportionality bias and agency panic, 20; QAnon movement, 19–21, 21–25, 22, 24; recommendations, 7 co-operation, with allies and partners, 63–64, 115–16, 170, 267, 269, 271
Cossette-Trudel, Alexis, 26–27
Counter-Terrorism Committee Executive Directorate (UN), 39
COVID-19 pandemic: cases and deaths in Canada and US, 250; vaccine distribution, 147. See also Canada’s intelligence and national security community and COVID-19 pandemic

COVID Alert (app), 131–32, 195–96

Criminal Code: authorities to collect information, 196, 198, 199, 207; on terrorism, 218, 224; on trade secrets, 205, 208n3
criminal justice system, 211–25; introduction and conclusion, 5–6, 211–12, 223–24, 262–63; comparison to deportation, 231; and extremism and terrorism, 215, 217–21, 224, 225n1; need for modernization, 223, 224–25; need for prioritization, 215–17, 224; overstretched system, 221–23; public health violators and, 215–16; recommendations, 9, 224–25; shifts in criminal offences and, 212–14; systemic racism and, 217
crisis informatics, 35
critical infrastructure: conspiracy theories and, 27; supply chain disruptions and, 52
critical infrastructure, and cyber attacks, 73–82; introduction and conclusion, 4, 73, 82, 264; attack impacts, 75–76; COVID-19 and, 78, 80–81; need for multi-stakeholder coordination against, 77–78; protection challenges, 78–80; recommendations, 7, 82; risk assessment of, 74–75; state responses, 76–77; vulnerability to, 74, 77. See also cybersecurity; cyberspace, and malicious non-state actors

CSE Act (Communications Security Establishment Act), 128, 130, 140, 200

CSIS Act (Canadian Security Intelligence Service Act), 197, 198–99, 206, 207
cyber attack operations, 132
Cyber Centre. See Canadian Centre for Cyber Security
cybersecurity: common threats, 129; COVID-19 challenges, 114–15; CSE operations, 127, 129–32. See also critical infrastructure, and cyber attacks; cyberspace, and malicious non-state actors
Cybersecurity and Infrastructure Security Agency (CISA), 76
cyberspace, and malicious non-state actors, 33–44; introduction and conclusion, 4, 33–34, 44, 263–64; Canada’s national security and, 42–43; delegitimation activities, 36–38; inciting violence and intimidation activities, 40–41; increase in extremist activities, 214–15; recommendations, 6–7; recruitment activities, 38–40; threats overview during COVID-19 pandemic, 35–36. See also critical infrastructure, and cyber attacks; cybersecurity

D
Daesh. See Islamic State of Iraq and Syria (ISIS) data: disparities for COVID-19 and racial and ethnic minorities, 252–54; Global Public Health Intelligence Network (GPHIN) and, 186–87. See also surveillance apparatus and data collection

Defence Intelligence Enterprise (DIE), 161–74; introduction and conclusion, 5, 161–63, 173–74, 266; adaptations for COVID-19, 164–67, 262; Canadian Forces Intelligence Command (CFINTCOM), 162, 167–73; counter-pandemic contingency plan, 163–64, 173, 262. See also Canadian Armed Forces; Canadian Forces Intelligence Command; Department of National Defence

Defense Information Systems Agency, 76

Defense Production Act (US), 56
defensive cyber operations (DCO), 132
delegitimation, 36–38
Democratic Republic of the Congo, 152–53
Denmark, 52, 76
Department of Defense (US), 76
Department of Health and Human Services (US), 255
Department of National Defence (DND): adaptations for COVID-19, 161–64, 262; counter-pandemic contingency plan, 163–64, 173, 262; CSE’s SIGINT operations and, 133; health intelligence and, 96; officer biographies, 156n2. See also Defence Intelligence Enterprise
departure, 231–42; introduction and conclusion, 6, 231–32, 265–66; 2022 deportation target, 242n4; administrative removals, 238–39; COVID-19 impacts on, 234, 235, 239–40; motions to stay, 237, 237, 242n2; process of, 233–34; recommendations on resuming post-pandemic, 240–42; serious, inadmissibility removals, 236, 242n1; voluntary removals, 236–38
de Wilde, Jaap, 98
disinformation, definition, 45n1. See also conspiracy theories; cyberspace, and malicious non-state actors
diversity, in supply chains, 54–56, 59
Domestic Policy Council, 256
Dosanjh, Ujjal, 179
Duarte, R v [1990], 197
dubajic, Daniel, 41

Index 275
early warning, 93, 96–97, 184–85, 186, 187–88, 270–71
economics: migrants and, 248; national security strategy for, 65–66
8chan, 21
Elections Canada, 267
Emergencies Act, 9, 194, 201–4, 206, 207, 208
Emergency Management Act, 78–79, 207
Emergency Management and Civil Protection Act (Ontario), 207
European Union, 34, 55, 63
Event 201 (pandemic tabletop event), 25
evil, problem of, 18
extremism, 214–15, 224. See also conspiracy theories; cyberspace, and malicious non-state actors; far-right extremism; terrorism
Eyre, Wayne, 146
far-left movements, 37
far-right extremism, 37, 39, 40, 214–15, 217–18, 263
Federal Emergency Management Agency (FEMA), 155
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), 90
Five Eyes partnership, 98, 102n4, 110, 134–35, 136, 140, 271
Flood, Colleen M., 203, 204
food banks, 61
food sector. See agriculture and food sector
foreign workers, temporary, 58, 63
Fortin, Dany, 147, 156n6
4chan, 19, 29n2
GeekWeek conference, 138
Germany, 16
Ghebreyesus, Tedros Adhanom, 35
Gioe, David V., 141
Global Affairs Canada (GAC), 96, 133, 169
global health governance, 188
global health security, 178, 179
Global Health Security Agenda (GHSA), 100–101, 102n4
Global Health Security Initiative, 182
globalization, 92, 93, 178
Global Outbreak Alert and Response Network (GOARN), 179, 181, 188
Global Public Health Intelligence Network (GPHIN), 177–89; introduction and conclusion, 5, 177–78, 188–89, 270; COVID-19 early warning and, 184–85; creation and expansion, 178–81; data challenges, 186–87; displacement of, 181–84;
Maersk, 76
malicious non-state actors. See cyberspace, and malicious non-state actors
manufacturing and production, 53–54, 58
Mapping and Charting Establishment, 171, 172
maritime operations, 149–50
Mayer, Anna, 206
McInerney v McDonald [1992], 204
medical intelligence (MEDINT), 168–69
Medicom, 54
Mehler Paperny, Anna, 225n1
Melley, Timothy, 20
mental health: law enforcement and mental health checkups, 217; in workplace during COVID-19, 111–12, 170, 267–68. See also workplace protection
Mexico, 37
Microsoft Teams, 81
migrant and refugee communities: introduction and conclusion, 6, 245, 262; background, 246; in Canada, 247, 247–48; COVID-19 financial, economic, and travel impacts, 248–49; COVID-19 public health impacts, 249–50; disparities in racial and ethnic data, 252–55; employment per service sector, 250, 251; and national and bilateral security opportunities, 255–56; recommendations, 8–9; socio-economic disparities, 251–52; in US, 246–48, 247
misinformation, definition, 45n1. See also conspiracy theories; cyberspace, and malicious non-state actors
Multinational Force and Observers (Sinai), 152
National Center for Medical Intelligence (NCMI), 93–94, 97
National Consortium for the Study of Terrorism and Responses to Terrorism (START), 16
National Defence Headquarters (NDHQ), 162, 164–67, 172. See also Defence Intelligence Enterprise
National Emergency Strategic Stockpile (NESS), 56–57, 65
National Institutes of Health, 263
National Research Council, 183
national security. See Canada’s intelligence and national security community and COVID-19 pandemic; national security operations
National Security Agency (NSA), 134, 136, 138
National Security and Intelligence Advisor, 10, 167
Integrated Terrorism Assessment Centre (ITAC), 136
intelligence: in Canada, 90, 96; collection challenges during COVID-19, 113–14; definition, 90; open-source, 118–19, 122, 267. See also Canada’s intelligence and national security community and COVID-19 pandemic; health intelligence; national security operations
Intelligence Assessment Branch (IAB), 118, 267
Intelligence Assessment Secretariat (IAS), 2, 90, 113, 117, 118, 169, 267. See also national security operations
International Health Regulations (IHR), 177, 180, 182
Internet. See critical infrastructure, and cyber attacks; cybersecurity; cyberspace, and malicious non-state actors
Investment Canada Act, 53
Iran, 75, 152
Islamic State of Iraq and Syria (ISIS), 37, 38–39, 40
Israel, 94, 95–96, 97, 98, 99, 194
IT services, 112–13
J
Jamieson, Kathleen Hall, 17
January 6, 2021 US Capitol attack, 7, 16, 21, 35, 40, 263
Joint Meteorological Centre, 170–71, 172
Jones, Scott, 131
Jordan, 152, 156n12
Jordan, R v [2016], 221, 222
K
Kallas, Jessica, 27
Kaplan, Alex, 23
Kosovo, 152
L
Laforest, Eric, 153
Lamberty, Pia, 17
Lametti, David, 221
Latvia (NATO Enhanced Forward Presence), 151–52, 153–54, 155, 166
Lebanon, 152, 156n12
lessons-learned exercise, 9–10
location data, 193–94, 198–99, 200, 204–6
long-term care facilities (LTCFs), 146–47, 148, 154
MacFarquhar, Neil, 38
MacKay, Peter, 225n1
Maersk, 76
malicious non-state actors. See cyberspace, and malicious non-state actors
manufacturing and production, 53–54, 58
Mapping and Charting Establishment, 171, 172
maritime operations, 149–50
Mayer, Anna, 206
McInerney v McDonald [1992], 204
medical intelligence (MEDINT), 168–69
Medicom, 54
Mehler Paperny, Anna, 225n1
Melley, Timothy, 20
mental health: law enforcement and mental health checkups, 217; in workplace during COVID-19, 111–12, 170, 267–68. See also workplace protection
Mexico, 37
Microsoft Teams, 81
migrant and refugee communities: introduction and conclusion, 6, 245, 262; background, 246; in Canada, 247, 247–48; COVID-19 financial, economic, and travel impacts, 248–49; COVID-19 public health impacts, 249–50; disparities in racial and ethnic data, 252–55; employment per service sector, 250, 251; and national and bilateral security opportunities, 255–56; recommendations, 8–9; socio-economic disparities, 251–52; in US, 246–48, 247
misinformation, definition, 45n1. See also conspiracy theories; cyberspace, and malicious non-state actors
Multinational Force and Observers (Sinai), 152
National Center for Medical Intelligence (NCMI), 93–94, 97
National Consortium for the Study of Terrorism and Responses to Terrorism (START), 16
National Defence Headquarters (NDHQ), 162, 164–67, 172. See also Defence Intelligence Enterprise
National Emergency Strategic Stockpile (NESS), 56–57, 65
National Institutes of Health, 263
National Research Council, 183
national security. See Canada’s intelligence and national security community and COVID-19 pandemic; national security operations
National Security Agency (NSA), 134, 136, 138
National Security and Intelligence Advisor, 10, 167
Index 277
National Security and Intelligence Committee of Parliamentarians, 10
National Security and Intelligence Review Agency, 10
national security operations, 107–25; introduction, 4, 107; accelerated change, 121; business continuity plans, 109–10; co-operation with allies, 63–64, 170, 271; costs of changes, 124–25; cybersecurity, 114–15 (See also cybersecurity); educating and understanding new audiences, 119–20; future implications, 120–25; information access challenges, 108–9; intelligence collection challenges, 113–14; IT services, 112–13; managing stress and anxieties, 111–12; methodology and study limitations, 107–8; new partners and clients, 115–16, 267, 269; new products, 117; new threat environment, 113; openness and public outreach, 121–22; open-source intelligence, 118–19, 122, 267; “ruthless prioritization” and readjustment, 116–17; staffing, 110–11; supply chain security, 114; widening scope, 123–24, 125; workplace flexibility, 122–23
National Security Policy (2004), 163, 173
National Strategy for Critical Infrastructure, 79
NATO, 102n4, 150, 152, 169, 170. See also Latvia (NATO Enhanced Forward Presence)
navy, 149–50
New Zealand, 102n2, 134, 136. See also Five Eyes partnership
Nigeria, 36, 92–93
Nordic Resistance Movement, 39
North Korea, 75, 76–77
NotPetya (malware), 75–76
Nstein Technologies, 180
Nuclear Threat Initiative, 179
O
Oath Keepers, 37
Oleksy, Tomasz, 17
Omand, David, 99
online activities. See critical infrastructure, and cyber attacks; cyberspace, and malicious non-state actors
Ontario: assistance from Canadian Armed Forces, 146, 148, 266; criminal justice backlog, 221; Emergency Management and Civil Protection Act, 207; migrant and refugee communities, 250; PPE manufacturing, 54
open-source intelligence, 118–19, 122, 267
Operation CALUMET, 152
Operation CARIBBE, 150
Operation CROCODILE, 152–53
Operation FREQUENCE, 151
Operation IMPACT, 152, 156n12
Operation KOBOLD, 152
Operation LASER, 146, 163–64, 262
Operation NEON, 150
Operation PRESENCE, 151
Operation REASSURANCE, 150–51, 166
Operation SOPRANO, 153
Operation UNIFIER, 152
Operation VECTOR, 147
P
Pacific NorthWest Economic Region, 256
Pauley, Justin-Philippe, 27
personal information. See surveillance apparatus and data collection
Personal Information Protection and Electronic Documents Act (PIPEDA), 198, 203, 204, 205
personal protective equipment (PPE), 53–57; introduction, 53; analysis and recommendations, 61–62, 100; challenges recognizing fraudulent PPE, 114; lack of redundancy, 56–57; limits to international co-operation, 63–64; manufacturing capacity, 53–54; supply chain diversity issues, 54–56; time frame issues, 56
personnel issues. See workplace protection
Pizzagate, 15
Plant, R v [1993], 197
point-of-entry removals, 235–36
Prime Minister’s Office (PMO), 133
privacy, 98–99, 196, 197–98, 203–4, 208. See also surveillance apparatus and data collection
Privacy Act, 196
Privy Council Office (PCO), 96, 133, 167. See also Intelligence Assessment Secretariat production and manufacturing, 53–54, 58
ProMED, 181, 184
proportionality bias, 20
Proud Boys, 37
Public Health Agency of Canada (PHAC): Canada’s intelligence and national security community and, 115, 116; creation of, 179; data disparities for COVID-19 and racial and ethnic minorities, 254–55; Global Public Health Intelligence Network (GPHIN) and, 100, 180, 182–83, 188; medical intelligence and, 169; National Emergency Strategic Stockpile (NESS) and, 57; partnership with US, 255; vaccine distribution, 147
public health violators, 215–16
Public Policy Forum, 121
S

S.A.B., R v [2003], 197
Sajjan, Harjit, 148
SARS, 179, 181, 185, 186
Scassa, Teresa, 203, 204, 208n2
Schecter, Anna, 40
secure compartmented information facilities (SCIF), 108–9, 110–11, 135, 136
serious, inadmissibility removals, 236, 242n1
Al-Shabaab, 36
Shared Services Canada, 129, 141n1, 266
Signals Directorate (Australia), 134
signals intelligence (SIGINT), 127–28, 132–35
Sinai (Multinational Force and Observers), 152
Singapore, 98–99, 195
Soberal, Derek, 40–41
social media, 17–18, 36–37, 40. See also conspiracy theories; cyberspace, and malicious non-state actors
Soleimani, Qassem, 152
Somalia, 36
Soufan Center, 38
South Korea, 195
South Sudan, 153
Speed, Shannon T., 78
Spencer, R v [2014], 197
staffing, 110–11. See also workplace protection
Statistics Canada, 254
Stewart, R v [1988], 205, 208n2
Stout, Mark, 141
stress and anxieties, 111–12, 267–68. See also workplace protection
Stuxnet (malware), 75
Sullivan, Jake, 255
Sullivan, Richard, 102n4
Supreme Court of Canada, 197, 203, 204, 205, 233
surveillance apparatus and data collection, 193–208; introduction and conclusion, 5, 193–94, 206, 269–70; Canadian Charter of

Taiwan, 55
Taliban, 36–37
Tam, Theresa, 184
Tech Against Terrorism, 42
technology, potential and limits of, 64–65
Telegram (app), 34, 37, 40
terrorism, 217–20, 224, 225n1, 231. See also
cyberspace, and malicious non-state actors; deportation; extremism

theodicy, 18
3M, 54, 55–56
Three Percenters, 37
time frames, in supply chains, 56, 60
trade secret, Criminal Code definition, 205, 208n3
TRADEWINDS, 150
Traffic Light Protocol, 118–19, 122
training, military, 171–72
teach, 248
Trudeau, Justin (Trudeau government), 57, 107, 164, 183, 201–2, 234, 255–56
Trump, Donald (Trump administration), 19, 24–25, 35, 55–56, 95, 247

Uganda, 151
Ukraine, 152
United Kingdom: COVID-19 conspiracy theories and, 27; cyber attack operations, 132; Government Communications Headquarters, 134, 136; personal protection equipment (PPE) and, 55; Quadripartite Medical Intelligence Committee and, 102n2. See also Five Eyes partnership
United Nations: Counter-Terrorism Committee Executive Directorate, 39
United States-Mexico-Canada Agreement (USMCA/CUSMA), 256
United States of America: bilateral opportunities with Canada, 255–56; COVID-19 cases and deaths, 250; COVID-19 health intelligence, 93–94, 95, 97; cyber attacks against, 75; data disparities for COVID-19 and racial and ethnic minorities, 252–54; health-care access disparities, 251–52; January 6, 2021 Capitol attack, 7, 16, 21, 35, 40, 263; migrant and refugee communities, 246–48, 247; Quadripartite Medical Intelligence Committee and, 102n2; remittances from, 249. See also Five Eyes partnership
urbanization, 92, 93

USS Theodore Roosevelt, 149

vaccine distribution, 147
Vigneault, David, 42
violence, online incitement, 40–41
voluntary removals, 236–38, 237

Wæver, Ole, 98
Walsh, P.F., 102n4
Wark, Wesley K., 96
Warner, Anthony Quinn, 15
Warner, Michael, 90
warning, early, 93, 96–97, 184–85, 186, 187–88, 270–71
Welch, Edgar Maddison, 15
World Bank, 249
World Health Organization (WHO): declaration of COVID-19 pandemic, 152, 164; future pandemics and, 92, 196; Global Outbreak Alert and Response Network (GOARN), 179, 181, 188; Global Public Health Intelligence Network (GPHIN) and, 179, 180–81; role in global epidemic intelligence, 177; underfunding, 178
Wu, Tong, 92

Youth Summit on Countering Violent Extremism Online, 42

Zadrozy, Brandy, 28n1
Zoom, 81
zoonoses, 92–93, 102n1
The emergence of COVID-19 has raised urgent and important questions about the role of Canadian intelligence and national security within a global health crisis. Some argue that the effects of COVID-19 on Canada represent an intelligence failure, or a failure of early warning. Others argue that the role of intelligence and national security in matters of health is—and should remain—limited. At the same time, traditional security threats have rapidly evolved, themselves impacted and influenced by the global pandemic.

*Stress Tested* brings together leading experts to examine the role of Canada’s national security and intelligence community in anticipating, responding to, and managing a global public welfare emergency. This interdisciplinary collection offers a clear-eyed view of successes, failures, and lessons learned in Canada’s pandemic response.

Addressing topics including supply chain disruptions, infrastructure security, the ethics of surveillance within the context of pandemic response, the threats and potential threats of digital misinformation and fringe beliefs, and the challenges of maintaining security and intelligence operations during an ongoing pandemic, *Stress Tested* is essential reading for anyone interested in the lasting impacts of the COVID-19 pandemic.

*Leah West*, SJD, is an Assistant Professor of International Affairs (Intelligence and National Security) at the Norman Paterson School of International Affairs at Carleton University.

*Thomas Juneau* is an Associate Professor in the Graduate School of Public and International Affairs at the University of Ottawa.

*Amarnath Amarasiningam* is an Assistant Professor in the School of Religion, and is cross-appointed to the Department of Political Studies, at Queen’s University.