Index

abstraction 58, 59–60, 61, 166
algorithms 58–61, 118, 119
Angell, I. 7, 15, 36, 42, 49, 50, 52, 74, 85, 97, 100, 114, 117, 165, 166
anonymity 7, 62, 149
anti-money laundering (AML) control 139
overview of global features 26, 28–31 research 36–7, 38, 39
three-level hierarchy 98–100
see also international anti-money laundering initiatives
anti-money laundering compliance 86, 140, 142
anti-money laundering compliance fear 22, 101, 114, 142
anti-money laundering information systems 128
see also case management system (CMS); CHIMERA system; profiling software; ZEUS profiling software
anti-money laundering law 11, 19, 29, 64, 129
anti-money laundering law enforcement 142
anti-money laundering policies 65, 67, 82
anti-terrorist financing 20, 21–2, 24, 27, 28, 31–5
see also Directive 2005/60/EC ‘approach’ 135–6 art 137, 138
artificial intelligence (AI) 117–18, 165
Ashby, W.R. 47–8, 54
asymmetry 37, 61, 78–84, 96, 109–10, 112, 113, 127, 131, 135
see also information asymmetry
ATM transactions 8, 85
Attacking the Profits of Crime (UN) 17, 22
attributes 92, 146–7, 157
auctions, and digital identities 10
audit trail 11, 12–13, 16, 51
Australia 14, 126, 167
Automated Centre for Transaction Recording 69, 70, 76, 166
Automated Message Switching System 19
automated suspicious transaction reports (STRs) 70, 82, 88, 101, 114, 166, 167
automation 117–19
automation/non-automation distinction 119, 120, 121, 125, 127, 128, 129–30, 132
autopoiesis 54, 56, 103, 107, 108, 109, 110, 111
avatars 9, 10
backlogs 67, 71, 82, 101, 123
bank accounts 74, 75–6, 77, 166
see also POSEIDON information system; ‘suspicious’ list of customer account numbers
bank secrecy 19
bank tellers, in Drosia bank case study 65, 72, 74, 76–7, 88, 90, 91, 93
banking risk management 23, 24, 25
banking supervision 17, 18, 23–5, 98, 139–41, 142, 160, 164
Basel Committee on Banking Supervision 17, 18, 23–5, 99, 139–40, 164
batch processing 90, 94
behavioural modelling 156–7
‘being at risk’ 133, 141
biological and chemical equipment sales 28
biology 54, 56, 117
blacklisting 20, 21, 26, 28–31, 166
bottom-to-top processes 116, 129, 131, 150, 151, 157
see also data-mining application of the risk-based approach
boundaries 41–2, 43, 47, 48, 49–50, 165
brain 46, 165
branch staff
and data-mining application of the risk-based approach 154, 159
and Drosia bank case study 65, 69–70, 71–2, 74, 75–7, 78, 79–84, 85, 88, 90, 91, 93, 123
branch supervisors/managers, in Drosia bank case study 91, 93
Brown, R. 14–15
bureaucracy 69–70, 96, 131–2, 143, 161
Case Management System (CMS)
and data-mining application of the risk-based approach 154, 155
and Drosia bank case study 63, 64, 72–4, 77–8, 79, 82, 84, 88, 89, 122
cash 7, 8, 10, 11, 15, 140–41, 143, 146–7
categorization
and data-mining application of the risk-based approach 155–6, 157
and observation 134, 135, 136
and risk-based approach 133, 135, 136, 137, 146–7, 160
and self-reference 58–9, 60, 61
cause-and-effect 39–40, 49, 51, 98, 101, 102, 138, 139
Cayman Islands 17, 20–21
central banks 6, 9, 11, 72, 82, 84, 87–8, 99
chaos, and systems theory 49–50, 52
CHIMERA system 63, 86–93, 94, 122, 123
China 8–9
civil liberties 22
closed systems 38, 160
closure, and technology 104, 111, 117, 121, 131, 132
coevolution 48, 52, 100, 102
coding
and functional differentiation of society 103
and systems theory 108–10, 111
and systems theory for anti-money laundering 110–14, 121, 122, 125, 127, 129, 130, 131
and technology as a system 116, 119, 120, 121, 125, 127, 128, 129–30, 132
cognition 46, 117, 165
see also non-cognition
collective intentionality 5–6, 9–10
commodity money 5, 6
Common Foreign and Security Policy (CFSP) 32, 87–8, 89, 91–2, 94, 122
communication
and coding 108, 110, 111–12, 113
and functional differentiation of society 103, 105, 106, 107
of risk representation 144–5
and systems theory 49, 50, 54
and systems theory for anti-money laundering (AML) 129, 131, 139
complexity
anti-money laundering systems 52, 150
audit trail in cyber laundering 12–13
audit trail in money laundering (ML) 16, 51–2
and data-mining application of the risk-based approach 151–2
and Drosia bank case study 69–71, 74–6, 85–6, 94, 96, 120
and functional differentiation of society 106
and money laundering (ML) models 150
organizations 38–9
and risk 136, 137, 146
and systems theory 45, 46, 47, 48, 49, 50, 51–4, 98, 116, 165
and systems theory for anti-money laundering (AML) 100, 101, 102, 113, 120–21, 122, 127, 129, 130, 131
technology 118, 127, 129, 130, 131
and uncertainty 136
see also complexity reduction; self-reference
complexity reduction
and data-mining application of the
risk-based approach 150, 151, 152, 155
and money laundering (ML) models
153–4
and risk-based approach 136, 143, 146
and systems theory 53–4, 55, 56
and systems theory for anti-money
laundering (AML) 123–7, 131, 139
and technology 117
computer programming languages 75, 89
computer programs 117, 118
confiscated proceeds of crime 17, 19, 25, 27, 34, 139
connectivity, and systems theory 52–4
Construction of Social Reality, The
(Searle) 5, 6, 102, 127
contingency, and systems theory 47, 48, 53, 56
crime money 6
control 48, 49, 98–9, 136, 139
corruption, and anti-money laundering 21, 28, 30
costs, in Drosia bank case study 66, 85–6, 87
Council of Europe 17, 25, 27
Countering Money Laundering Plan
of Action (UN) 22
Coward, L.A. 46
criminality 11, 13, 18–19, 22–3, 25, 106
crown dependencies, United Kingdom 20–21, 28–9
customer due diligence 23, 24, 25, 164
customer identification numbers, in
Drosia bank case study 74, 75–7, 120–21
customer identity 64, 65, 69, 74, 75–7, 92, 120, 149
customer information 64–5, 69, 74, 75, 76–7
customer information deficits 76, 77
cyber laundering 12–13, 15
cybernetics 54, 56, 116
data-mining application of the risk-based approach 148–61
data protection law 65
database structures, in Drosia bank case study 75
Davies, G. 5, 6
decomposition 41, 43–4, 45–6, 52, 98, 120
demographic data, and data-mining application of the risk-based approach 158, 159, 160
developing countries, digital identity creation 10
differentiation see distinction/difference; functional
differentiation of society
digital identities 9, 10
Directive 2001/97/EC 18, 26, 27
Directive 2005/60/EC 2, 18, 26, 28, 139–44
Directive 2008/20/EC 18, 26
discrimination, and profiling in terrorist financing 32
disintermediation, and cyber-laundering 12–13, 15
distinction/difference
and data-mining application of the risk-based approach 152–3, 158
and observation 117, 118
and systems theory 41–5, 46, 47, 48, 49, 51, 52, 53, 61, 108–10, 111, 165
and systems theory of anti-money laundering (AML) 100, 111, 112–13, 119–20, 122, 130
see also automation/non-automation distinction; legal/non-legal distinction; prosecution/non-prosecution distinction; suspicious/non-suspicious distinction
Ditton, J. 14–15
Drosia bank case study
access to the bank 62–4
automated profiling software 63, 64–5, 84–7, 93–5, 123
broader comments 95–6
CHIMERA information system 63, 86–93, 94, 122, 123
Electronic Updates System (EUS) 93
examining scenarios 68–74
genral comments about the bank 64–8
POSEIDON information system 63, 74–8, 87, 88, 90, 91–2, 94, 119–21, 122, 166
suspicious transaction reports, asymmetry of 78–84, 96
and systems theory for anti-money laundering (AML) 113, 119–21, 122–3, 128
drug trafficking 13, 14, 26
see also Countering Money Laundering Plan of Action (UN); Political Declaration on Global Drug Control at the UN General Assembly; Vienna Convention (UN)
e-cash 7, 8, 10, 11, 15
e-transactions 15, 85, 161
economic growth 15–16, 22
economic subsystem 105, 106
economic system 104–5, 106, 107, 109
Egmont Group 22, 163
electreaucracy 131–2, 161
Electronic Updates System (EUS) 63, 93
elements 44, 46, 52–4, 56, 107, 165
e emergence and artificial intelligence (AI) 165
and functional differentiation of society 106
and game theory 165
and systems theory 40–41, 45, 47, 52, 53
and systems theory for anti-money laundering (AML) 100, 101, 122, 126, 129, 130
and technology as a system 122, 129, 130, 144
England, C. 7, 163
Entropia Universe 8
entropy 50, 165
environments and coding 110
and organizations 38–9
and systems theory 41–3, 44–5, 47–9, 50–51, 53, 55, 56, 135, 165
and systems theory for anti-money laundering (AML) 100, 112
and technology as a system 119
see also social construction of reality errors, and self-reference 59, 60
European Central Bank 11
European Commission 2, 18, 26, 27, 28, 139–44, 148, 166
European Community 18, 27
European Economic Commission 11, 17, 18, 25–6, 27
European Union (EU) 2, 11, 17, 18, 25–6, 27, 28, 87–8, 98, 139–44, 148, 166
external (exoteric) system/environment relations, and systems theory 45
external money laundering investigation requests, in Drosia bank case study 68–71
extinction, and systems theory 50
falsehood 101–2, 137
fantasy equality 14–15
Fast Transmission of Electronic Messages (FTEM) system 63, 69, 77, 90, 121, 122
feedback 49–50, 52, 131, 144–5, 147–8, 153, 159
see also negative feedback; positive feedback
fi at money 6–7
Financial Action Task Force (FATF) 12, 14, 17, 18, 20–22, 24, 25, 26, 27, 28–33, 99, 163, 164
Financial Intelligence Units (FIUs) and corruption 21
and data-mining application of the risk-based approach 152, 159
and Drosia bank case study 66–7, 68–71, 82
information exchange 22, 24
suspicious transaction reports (STRs) and prosecutions ratio 123–7
and systems theory for anti-money laundering (AML) 99, 131
United Kingdom 70, 101, 167
Financial Services Authority (UK) 142, 148, 166
financial transactions see transactions
flexibility 40, 48, 55, 56, 140
forms, and technology 116
Foucault, M. 54
Fowler, G. 8–9
function 103, 107–8, 110
function-systems 105–7, 115–16
see also economic system; legal system; political system
functional differentiation of society 102–8, 109, 110
functional simplification, and technology 117, 118, 121, 127, 132
funding, of intelligence agencies 34, 35
G7 countries 20, 26
game theory 165
Geyer, F. 55–6
Gilmore, W. 12, 18, 19, 25
globalization 15–16, 22
goals, and systems theory for anti-money laundering (AML) 100–101
gold 5, 6
government money 8–9, 10, 12
government regulation, and e-money 7, 9
governments, criminality definitional differences 11
‘grand theories’ 38
Granville, J. 15
handwriting 58–61, 70, 72
Hawala 6, 163
Hayek, F. von 9
hazards, and risk 133, 141
hierarchies, and anti-money laundering (AML) 98–100
‘high-risk’ 25, 140–41, 146–7
‘holistic’ approach 31, 40, 41, 126, 164
human activity systems 125, 127, 139, 143–4
human observers 117–18
human profiling 35, 88
human rights 25, 27
identity see customer identity; digital identities
illegality see criminality; legal/non-legal distinction
in-house software development see CHIMERA system; POSEIDON information system
infinite regression 42, 165
inflexibility, of software in Drosia bank case study 73
information 34, 35, 157–8, 159
see also customer due diligence; customer information; customer information deficits; information dissemination; information processing; information systems; international information exchange; Know Your Customer (KYC); Know Your Customer policies; knowledge; quality of information; quantity of information; statistical information
information asymmetry 34
information dissemination 93
information processing 36, 58–61
information systems 25, 39, 57, 58, 128–9, 139, 140, 141, 143
see also Case Management System (CMS); CHIMERA system; Fast Transmission of Electronic Messages (FTEM) system; Managing Information Systems (MIS) Department; POSEIDON information system; technology; ZEUS profiling software
instances, and self-reference 58–9, 60
institutional facts 5, 7
integration, in three-stage model of money laundering 12
intellectual structure, and risk transformation from uncertainty 133
intelligence 88, 117–18, 143
intelligence agencies 21, 28, 33, 34, 35, 131
interactions and risk 136, 137
and social construction of reality 127–8
and systems theory 40, 45, 48–9, 51, 52
and systems theory for anti-money laundering (AML) 100, 101, 119–23, 127, 130, 131, 139
and technology as a system 119
internal (esoteric) system/environment relations, and systems theory 45
international anti-money laundering initiatives 16–18
see also Attacking the Profits of Crime (UN); Basel Committee on Banking Supervision; Council Directive 91/308/EEC; Directive 2001/97/EC; Directive 2005/60/EC; Directive 2008/20/EC; Financial Action Task Force (FATF); Political Declaration and Action Plan Against Money Laundering (UN); Political Declaration on Global Drug Control at the UN General Assembly; United Nations Convention Against Transnational Organized Crime; Vienna Convention (UN)
international cooperation, and Countering Money Laundering Plan of Action (UN) 22
international information exchange 22, 24, 25, 29, 164
international information networks, and anti-money laundering 22
International Monetary Fund (IMF) 13, 15, 21, 30–31, 98, 99
Internet, and cyber laundering 12–13, 15
Internet companies 8, 28
interoperability deficits of software, in Drosia bank case study 86, 89–90, 91–3, 94
interoperability of software, in Drosia bank case study 87–8, 89
interpenetration of systems 100–101, 106, 110, 116, 119, 120, 121, 128
investment, and virtual currencies 10, 11–12
‘islands of reduced complexity’ see complexity reduction
Johnson, J. 21, 29
Know Your Customer (KYC) 9, 15, 22, 23, 24, 25, 164
Know Your Customer (KYC) policies 64–5, 87, 88, 94
knowledge 138–9
Korzybski, A. 54
labour exploitation, and digital identity creation 10
language 42, 54, 57–8, 90–92, 122
large sums of money 32, 33, 140–41, 143
Latin characters, and Drosia bank case study 90–92
laws see anti-money laundering law; anti-money laundering law enforcement; data protection law
layering, in three-stage model of money laundering 12
legal/non-legal distinction 108–9, 110, 113, 125
legal subsystem 105, 106, 110, 125
legal system 104–5, 106, 107, 108–9, 110, 113, 125, 139
Lilley, P. 13, 15, 26, 28, 29–30
linear processes 99–100, 105, 118, 121
‘little theories’ 38
local stakeholders, and anti-money laundering (AML) hierarchies 99
logic 40, 117, 118, 138
‘low risk’ 141, 146, 147
machine observers 117–18
Managing Information Systems (MIS) Department 75, 76, 85–7, 88, 89
manual processes
and data-mining application of the risk-based approach 152, 154, 159, 161
and Drosia bank case study 69–70, 71–2, 75, 83, 89, 94–5
Index

and money laundering (ML) models 150
and systems theory for anti-money laundering (AML) 122, 125
see also human activity systems; human profiling
mathematical self-reference 55
matrix-based risk attributes 146–7
Maturana, H. 48, 54
meta-systems, and systems theory 42
Mitleton-Kelly, E. 51
MMORPGs (Massive Multiplayer Online Role Playing Games) 8–10, 12
Moeller, H.-G. 102–3, 109
Mohamed, S. 11, 20, 22, 28
money, nature and functions 5–12
money laundering
and collective intentionality 6, 163
complexity 51–2
criminility definition, differences between nation laws 11
definitions 7, 13, 18–19, 22–3, 25
models 12, 60–61, 150–51, 153–5, 156–7
nature of laundered money 5–12
process 12–13
structural coupling with anti-money laundering (AML) 100, 102, 108, 129
typologies 12–13, 28, 36, 65, 72, 87, 157
Money Laundering Analysis Teams (MLATs)
and data-mining application of the risk-based approach 152, 154, 160
and systems theory for anti-money laundering (AML) 122, 123
money laundering markets, estimation problems 13–16
Money Laundering Reporting Officers (MLROs) 63–4, 65–6, 72, 82, 83, 153, 160
monitoring
and anti-money laundering effectiveness 98, 99, 144, 146
and suspicious transactions 25, 29, 63, 84, 85, 87, 88, 90, 112–13, 140, 161
and terrorist financing 33, 34, 35
multi-disciplinary research 36–7, 38, 39
national language character set
conversion 91–2, 122
national laws, criminality definitional differences 11
national organizations, and anti-money laundering (AML) hierarchies 99
nationality 91–2
nations, geographical spread of terrorism 34
Nauru 21, 28–9, 30
Naylor, R. T. 21
negative feedback 50
negentropy 50, 165
Nietzsche, F. 42, 54, 165
non-bank financial institutions’ supervision 23, 27
non-cognition 118
non-compliance, Financial Action Task Force (FATF) 20–21
Non Cooperative Countries and Territories (NCCT) 88
non-hierarchical organization 99–100, 104, 105–6
non-linear processes 50, 99–100, 104, 105–6, 135
non-observation 51, 53, 109–10, 119, 134–5, 137
norms 13, 98, 99–100, 103
observation
and cause-and-effect 39–40
and data-mining application of the risk-based approach 157–8
and non-observation 134–5
and risk 133, 135, 139
and risk-based approach 135, 136
and systems theory 37, 40, 41, 42, 43, 45, 47, 48, 51, 53, 57, 98, 109–10, 116, 152
and systems theory for anti-money laundering (AML) 101–2, 126, 129
and technology as a system 117–18, 119, 130
see also non-observation
off-the-shelf automated profiling solutions, and Drosia bank case study 85–7
Office of Foreign Assets Control (OFAC) 32, 34, 87–8, 91–2, 94, 122
offline processing, in Drosia bank case study 73, 90, 94
online games 8–10, 12
open systems 38–9
operational risk 139–40
opportunities, and ‘taking a risk’ 133, 141
organizations 38–9, 106
organized crime 26, 27
see also United Nations Convention Against Transnational Organized Crime
outsourcing 10
see also Case Management System (CMS)
paradigm shifts, and systems theory 37–8
parameterization 142–3, 150, 154–5
Parkman, T. 33
pattern recognition algorithms 58–61
payments 5, 15
Pelling, G. 33
Pentagon 21, 28
Pinter, H. 101, 137
placement, in three-stage model of money laundering 12
plans of action, and risk 133–4
police, and anti-money laundering 19
Political Declaration and Action Plan Against Money Laundering (UN) 20
Political Declaration on Global Drug Control at the UN General Assembly 22
political (sub)system 104–5, 106–7, 109
politics, and anti-terrorist financing 32, 33–5
POSEIDON information system 63, 74–8, 87, 88, 90, 91–2, 94, 119–21, 122, 166
positive feedback 49–50, 101, 103, 158
power 98–9, 106
privately-issued virtual currencies 7, 8–9
probabilities 58, 141–2, 146, 147, 155–6
problem solving 39–40, 116
professional secrecy, and Directive 2001/97/EC 26, 27
profiling rules, and Drosia bank case study 87
profiling software 32–3, 35, 64–5, 84–7, 150, 151, 153, 159, 160–61
see also ZEUS profiling software
profiling terrorist financing 32–3, 34, 35
prosecution/non-prosecution distinction 125
prosecutions 113, 123–7
prosecutors, and Drosia bank case study 68–71
punishment, and serious crime 23
Qin, J. 8–9
QQ coins 8–9
qualitative assessment of risk 139–40, 141–2, 147
quality, and systems theory 46
quality of information 66–7, 78, 82–4, 95, 153
quantitative assessment of risk 139, 141–2
quantity, and systems theory 46
quantity of information
and data-mining application of the risk-based approach 149–50, 151–2, 153, 155, 161
suspicious transaction reports and Drosia bank case study 65–7, 70, 71, 78, 79–83, 88, 94–5, 123, 131
suspicious transaction reports and prosecutions ratio 123–7
suspicious transaction reports in the United Kingdom 70, 101, 114, 166, 167
queries 60, 76, 150, 151, 154, 166
rationality 40, 138
real economy, money laundering’s contribution 14
reality 5, 102, 127–8, 135, 138
reduced risk of money laundering (ML), and Directive 2005/60/EC 140
reductionism 40, 41, 45, 46, 136
reference numbers, in Drosia bank case study 73–4
reference state, and systems theory 50
regenesis of risk 137–8, 147–8
relations, and systems theory 44, 45, 46, 52, 56, 107
reporting to central bank, in Drosia bank case study 72
representation 133–4, 135, 137–8, 144–5
reputation of bank, in Drosia bank case study 65
requirements specifications of software, in Drosia bank case study 73, 85–6, 87–8
research, anti-money laundering 36–7, 38, 39
RFID (Radio Frequency Identification) microchips 11
Rider, B. 21, 28
risk
and anti-money laundering (AML) 139
and coding, in systems theory for anti-money laundering (AML) 113–14
and complexity 136, 137, 146
concept 138–9
deconstructing 133–6
in Drosia bank case study 65, 77, 83–4, 89
levels 140–42
money laundering in Drosia bank case study 65
and observation 133, 135, 139
regenesis 137–8, 147–8
and systems theory 53
and uncertainty 133–4, 135, 136, 138, 139, 142
risk assessment 141, 144
risk attributes 146–7, 157
risk-based approach
and categorization 133, 135, 136, 137, 146–7, 160
and complexity reduction 136, 143, 146
and construction of risk-deconstruction 145–8
and corruption 29
data-mining application 148–61
and Directive 2005/60/EC 26, 28, 139–44
and Drosia bank case study 83, 84
models 145–6
and observation 135, 136
risk-based supervision 140–41, 142, 160
risk-defined parameters 142–3
risk-defined profiles 141, 143, 157, 158–9
risk management 89, 136, 140, 141, 144
risk representation 133–4, 137, 144–5, 160
risk scores, and automated profiling in Drosia bank case study 95
risk-sensitivity 141, 143
risk-subsystems 136, 137, 147
Robinson, Philip 142
Rossbach, S. 39, 53, 54, 147
Roule, T. 21, 29
Salak, M. 21, 29
sanctions 29
Searle, J. 5, 6, 102, 127–8
Second Life 8
security 76–7, 149
security risk 77
selection 47, 53–4, 55, 56, 136, 154–5
self-observation, and systems theory 56
self-organization 49, 52, 54, 104, 107
self-reference
and asymmetry 61, 110
and coding 109–10, 113
and functional differentiation of society 107
and risk 137, 139, 160
and systems theory 43, 53, 54–61, 103, 152
and systems theory for anti-money laundering (AML) 100, 106, 107, 113, 114
and technology as a system 56–7, 118–19
serious crime, UN definition 23, 27
serious suspicious transaction reports (STRs), and Drosia bank case study 67
shell banks 16, 24, 30
‘significant flexibility’, and Directive 2005/60/EC 140
small sums of money 33
Smithson, S. 50, 74
social construction of reality 5, 102, 127–8
social systems 57
society 102–8
specificity, and self-reference 59
spontaneity, human versus machine observers 117, 118
stability, and systems theory 48, 50, 52
stakeholders
and anti-money laundering (AML) 1–2, 28, 98–100
and anti-terrorist financing 31–2, 35
and data-mining application of the risk-based approach 159, 160
and Drosia bank case study 63–4, 78, 95
and risk-based approach 136, 144–5, 147–8
and systems theory for anti-money laundering 101, 112, 113, 114, 129, 131, 139, 144–5
and technology as a system 1–2, 119
statistical information 72, 73
store of value 5, 9, 12
structural changes, and systems theory 48–9
structural coupling
and systems theory 48–9, 135, 137, 166
and systems theory for anti-money laundering (AML) 100, 102, 108, 125, 129
and technology 120, 132
subsystems
and coding 108, 110, 111
and functional differentiation of society 102–8
and systems theory 41, 44, 45, 49, 50, 56
and systems theory for anti-money laundering (AML) 14, 100, 101, 105–8, 145
see also economic subsystem; legal subsystem; political subsystem; risk-subsystems; technological subsystem
supervision 23, 27, 98, 140–41, 142, 160
see also Basel Committee on Banking Supervision
surrealism 137, 138
‘suspicious’ list of customer account numbers 153, 154, 155–6, 158
‘suspicious’ lists of names 87–8, 89, 90–92, 94, 122
suspicious/non-suspicious distinction coding in systems theory for anti-money laundering 111–12, 113, 114, 121, 122, 129, 130, 131
and risk-based approach 141, 143
suspicious transaction monitoring 25, 29, 63, 84, 85, 87, 88, 90, 112–13, 140, 161
suspicious transaction reports (STRs) and cyber laundering 13
and data-mining application of the risk-based approach 148–9, 152–3, 154, 158, 159, 160, 161
and Directive 2005/60/EC 28
and Drosia bank case study 64, 65–7, 71–2, 78–84, 87, 88, 90, 94–5, 96
and prosecutions ratio 123–7
and systems theory of anti-money laundering (AML) 113–14, 122, 123
United Kingdom 70, 101, 114, 166, 167
SWIFT messaging 90–91, 122
system, in systems theory 43–7, 57–8, 98–102
see also closed systems; economic system; function systems; human activity systems; legal system; meta-systems; open systems; political system; social systems; subsystems; technical systems
Index

systemic reformation, and systems theory 50
systemic survival 2–3, 50, 56, 103
systems theory
and coding 108–10, 111
and complexity 45, 46, 47, 48, 49, 50, 51–4, 98, 116, 165
and functional differentiation of society 102–4
overview 37–41
and risk deconstruction 133–6
and self-reference 43, 53, 54–61, 103, 152
and the system 43–7, 57–8, 98
and technology 56–7, 115–19, 125, 129–30, 132, 143–4
see also boundaries; complexity; complexity reduction; distinction/difference; Drosia Bank case study; environments; systems theory for anti-money laundering (AML)
systems theory for anti-money laundering (AML)
coding 110–14, 121, 122, 125, 127, 129, 130
and Drosia bank case study 113, 119–21, 122–3, 128
functional differentiation of society and the role of AML 102–8
‘islands of reduced complexity’ 123–7, 131, 139
and risk 139
the system 98–102
technological construction of AML-reality 103, 128–32
and technology 115–23, 125, 126, 127, 132, 143–4
see also data-mining application of the risk-based approach
‘taking a risk’ 133, 141
Tanzi, V. 12, 14, 21
tautology 37, 56, 61, 109–10, 141
‘technical criteria’ 141, 143
technical systems 57–8
technological construction of AML-reality 103, 127–32
technological subsystem 130, 131
technology
coding 116, 119, 120, 121, 125, 127, 128, 129–30
as a form 116
self-reference 56–7, 118–19
as a system 56–7, 115–19, 125, 129–30, 132, 143–4
and systems theory for anti-money laundering (AML) 115–23, 125, 126, 127, 143–4
terrorism 21, 32–4
terrorist financing 32–3, 34, 35
see also anti-terrorist financing
terrorist organizations 33, 34
time factors
bank account, age in Drosia bank case study 75
branch staff time in Drosia bank case study 70, 71, 76, 77, 88, 93, 121
in data-mining application of the risk-based approach 149, 151, 154
FIU staff time in Drosia bank case study 67, 71, 101
MLAT staff time in Drosia bank case study 82, 95, 123
suspicious transaction reports (STRs), age in Drosia bank case study 90
transaction data, age in Drosia bank case study 68–70, 94
top-to-bottom processes 104, 116, 129, 131, 132, 150, 153
trade openness, and economic growth 15–16
training, in Drosia bank case study 65–6, 82, 88
transaction codes, in Drosia bank case study 90
transaction slips, in Drosia bank case study 69–70
transactions 32, 33, 60, 68–71, 74, 90, 140–41, 143
see also ATM transactions; Automated Centre for Transaction Recording; data-mining application of the risk-based approach; e-transactions;
suspicious transaction reports (STRs)  
transcendental property, and data-mining application of the risk-based approach 152  
transnational organizations, and anti-money laundering hierarchies 98–9  
triality, and systems theory 41–2, 165  
True Positive Rate (TPR) 95, 148–9, 153, 159, 161  
trust 6–7, 9, 163  
th 101–2, 111, 112, 137  
uncertainty 133–4, 135, 136, 138, 139, 142  
underground economy, and money laundering estimation problems 14, 15, 16  
United Kingdom 6, 20–21, 28–9, 34, 70, 101, 114, 166, 167  
United Nations (UN) 13, 17–19, 20, 22–3, 24, 27, 98, 99, 164, 166  
United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 17, 18–19, 20, 27  
United States 20, 21, 28, 29, 87–8  
universe 42  
unsuccessful suspicious transaction reports (STRs), and Drosia bank case study 82–3  
updating ‘suspicious’ lists of names, and Drosia bank case study 89  
Varela, F. 48, 54  
variety 47–8, 49, 100  
Vienna Convention (UN) 17, 18–19, 20, 27  
virtual currencies 8–10, 12  
virtual goods 8, 12  
virtual identities 9, 10  
Walker, J. 13, 14  
‘whole’ 40, 45, 46, 104, 126, 134–5, 136, 138  
see also ‘holistic’ approach  
World Bank 16, 30  
ZEUS profiling software 63, 93–5, 123