

# Inhaltsverzeichnis

<b>1</b>	<b>Soziologische Grundlagen . . . . .</b>	<b>1</b>
1.1	Kommunikationspsychologische Grundlagen . . . . .	1
1.1.1	Anonyme Kommunikation . . . . .	2
1.1.2	Das Vier-Seiten-Modell der Kommunikationspsychologie . . . . .	3
1.1.3	Die vier Dienstleistungskommunikationsprozesse . . . . .	5
1.1.4	Probleme auf der Beziehungsebene . . . . .	6
1.1.5	Probleme bei der Selbstkundgabe . . . . .	7
1.1.6	Möglichkeiten der menschlichen Kommunikation . . . . .	8
1.1.7	Digitale Kommunikationsprothesen . . . . .	9
1.1.8	Netzaufbau nach dem menschlichen Verständnis . . . . .	11
1.1.9	Erweitertes Vier-Seiten-Modell der Kommunikation 4.0 . . . . .	13
1.1.10	PDS als Weiterentwicklung eines Softwareagenten . . . . .	16
1.1.11	Der Anfrageprozess . . . . .	17
1.1.12	Der Bestell- und Bezahlprozess . . . . .	19
1.1.13	Der Empfehlungsprozess . . . . .	20
1.1.14	Angepasste M2M-Kommunikation . . . . .	21
1.1.15	Berücksichtigung der Stärken der Gesprächspartner . . . . .	23
1.1.16	Chancen durch das Aufbrechen der Wertschöpfungsketten . . . . .	25
1.1.17	Fazit . . . . .	26
1.2	Convenience unter Berücksichtigung des demografischen Wandels . . . . .	27
1.2.1	Die Alterspyramide . . . . .	28
1.2.2	Die überzogene Selbsteinschätzung der Deutschen . . . . .	28
1.2.3	Datenschutzprioritäten aus Sicht eines Angreifers . . . . .	30
1.2.4	Convenience und Sicherheitsbewusstsein . . . . .	31
1.2.5	Jung-hilft-Alt-Konzept . . . . .	34
1.2.6	Höchste technische Sicherheit versus erprobte adaptierte Sicherheit	34
1.2.7	Symmetrische Verschlüsselung versus asymmetrische Verschlüsselung . . . . .	35

---

1.2.8	Akzeptierte Datenspeicherung mit akzeptabler Sicherheit . . . . .	37
1.2.9	Dezentralisierte akzeptierte Währungen . . . . .	39
1.2.10	Dezentrale Kommunikation . . . . .	41
1.2.11	Fazit . . . . .	43
<b>2</b>	<b>Rechtliche und organisatorische Grundlagen . . . . .</b>	<b>45</b>
2.1	Vorratsdatenspeicherung . . . . .	45
2.1.1	Vereinbarkeit von Strafverfolgung und Datenschutz . . . . .	46
2.1.2	Eignung der Richtlinie . . . . .	46
2.1.3	Erforderlichkeit und Verhältnismäßigkeit – Differenzierung nach Art der erhobenen Daten . . . . .	47
2.1.4	Auswirkungen auf Big Data . . . . .	48
2.1.5	Auswirkungen auf Webanalysen . . . . .	49
2.1.6	Beschränkung des überwachten Personenkreises . . . . .	49
2.1.7	Beschränkung der Zugriffsrechte der nationalen Behörden . . . . .	49
2.1.8	Festlegung des Speicherzeitraums . . . . .	49
2.1.9	Schutz gespeicherter Kommunikationsdaten . . . . .	49
2.2	Verbesserung der Compliance . . . . .	50
2.2.1	CMS-Systeme alleine reichen nicht . . . . .	50
2.2.2	Nicht lösbarer Problemstellungen . . . . .	50
2.2.3	Forderungen an die Wirtschaft . . . . .	51
2.3	Neustrukturierung der ICANN/IANA . . . . .	51
2.3.1	Ausgangssituation . . . . .	51
2.3.2	Forderungen aus Sicht des Trusted Web 4.0 . . . . .	52
2.3.3	Trusted Web 4.0 mit eigener TLD . . . . .	52
2.3.4	Forderungen an die IANA . . . . .	53
2.4	Optimale Umsetzung des europäischen Urheberrechts und Datenschutzes . . . . .	53
2.4.1	Freier Zugang zu Information versus Urheberrecht . . . . .	54
2.4.2	Forderungen an den Gesetzgeber . . . . .	55
2.5	Empfehlungen für die Informationssicherheit gemäß ISO 27001 . . . . .	56
2.5.1	Die Situation in der Informationssicherheit . . . . .	56
2.5.2	Zukünftige Angriffe werden interdisziplinär . . . . .	58
2.5.3	Zukünftige Angriffe werden mehrstufig . . . . .	59
2.5.4	Ideologische Dimension der Zentralisierung . . . . .	62
2.5.5	Gesamtkonzept der IT auf dem Prüfstand . . . . .	62
2.5.6	Formen der Dezentralisierung . . . . .	65
2.5.7	Bring your own device (BYOD) . . . . .	67
2.5.8	Einführung von Trusted Web 4.0 in Institutionen . . . . .	69
2.5.9	Dezentrale Webseitendistribution zum Entnetzen von Servern . . . . .	72
2.5.10	Voraussetzung für den Aufbau einer dezentralen (Notfall-)Organisation . . . . .	73
2.5.11	Planung und Konzeption einer dezentralen (Notfall-)Organisation	76

---

2.5.12 Sieben-Stufen-Modell für Cyberangriffe . . . . .	77
2.5.13 Strukturiertes Vorgehen in vier Schritten . . . . .	79
2.5.14 Neue Vorgaben zur Informationssicherheit für große Institutionen . . . . .	88
2.5.15 Notfallplanung in der IT . . . . .	92
2.5.16 Neustrukturierung des Bundestagsnetzwerks . . . . .	94
2.5.17 Der Gewinner des Cyber Wars . . . . .	97
2.5.18 Fazit . . . . .	98
<b>2.6 Demokratiekonforme Anonymisierung und Strafverfolgung . . . . .</b>	<b>99</b>
2.6.1 Neue Möglichkeiten des Terrorismus aus Sicht der Angreifer . . . . .	100
2.6.2 Kampf um den Erhalt der Bürgerrechte . . . . .	102
2.6.3 Effekte von Massenüberwachung und zentraler Datenhaltung . . . . .	104
2.6.4 Bessere Überwachung der potenziellen Tätergruppe . . . . .	106
2.6.5 Stärkung der Freiheitsrechte der Bürger . . . . .	106
2.6.6 Das Problem der Anonymisierung von Daten . . . . .	107
2.6.7 Sechs Stufen zur Standardisierung von Anonymisierungsprozessen . . . . .	109
2.6.8 Kommunikation in dezentralen Netzen gemäß Personalisierungsstufe 4 . . . . .	111
2.6.9 Justiziable Beweiskraft . . . . .	113
2.6.10 Digitale Forensik in dezentralen Netzen . . . . .	114
2.6.11 Transparenz zum Schutz von Bürgerrechten . . . . .	116
2.6.12 Durchsetzungsfähigkeit . . . . .	116
2.6.13 Fazit . . . . .	117
<b>3 Der Bauplan der Zukunft . . . . .</b>	<b>119</b>
<b>3.1 Veränderung der Wertschöpfungsprozesse . . . . .</b>	<b>119</b>
3.1.1 Situation und Perspektive des Kommunikationsnetzmarktes . . . . .	120
3.1.2 Forderungen für den Aufbau europäischer Multimedianetze . . . . .	121
3.1.3 Social Media als Treiber der Datenverwertung . . . . .	122
3.1.4 Onlinewerbung versus klassische Werbung . . . . .	125
3.1.5 Neue Wertschöpfung durch dezentralisierte Funknetze . . . . .	128
3.1.6 Finanzierbarkeit eines dezentralisierten Mobilfunknetzes . . . . .	129
3.1.7 Fazit . . . . .	132
<b>3.2 Persönliches digitales System als disruptive Technologie . . . . .</b>	<b>133</b>
<b>3.3 Ausblick in die einzelnen Bereiche . . . . .</b>	<b>134</b>
3.3.1 Anonymisierte E-Health-Systeme . . . . .	134
3.3.2 Unterstützung statt Überwachung im vernetzten Auto . . . . .	136
3.3.3 Homebot zur Verwaltung von Smart Home und zur Energieversorgung . . . . .	140
3.3.4 Dezentrales E-Government . . . . .	141
3.3.5 Industrie 4.0 als intelligentes Netzwerk von Maschinen . . . . .	143
3.3.6 Der Logistiker 4.0 als regionale Clearingstelle . . . . .	144
3.3.7 Dezentralisierung des Finanzwesens . . . . .	145

3.4	Geht nicht, gibt es nicht! . . . . .	147
3.4.1	Unternehmensführung ohne Veränderung . . . . .	150
3.4.2	Unternehmensführung mit aktiver digitaler Transformation . . . . .	151
3.4.3	Unternehmensführung mit Dezentralisierung und Anonymisierung . . . . .	151
3.5	Die nächsten Schritte . . . . .	152
3.5.1	GISAD . . . . .	154
3.5.2	Forschungsprojekte für ein persönliches digitales System . . . . .	156
3.6	Cloud ab 2020 – Dezentralisierte Softwareentwicklung . . . . .	162
<b>Checkliste für die digitale Transformation . . . . .</b>		165
<b>Literatur . . . . .</b>		169
<b>Sachverzeichnis . . . . .</b>		177