Miron Lakomy

Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw

WYDAWNICTWO
UNIWERSYTETU ŚLĄSKIEGO
KATOWICE 2015

Cyberprzestrzeń
jako nowy wymiar rywalizacji
i współpracy państw

NR 3293

Miron Lakomy

Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw

Wydawnictwo Uniwersytetu Śląskiego • Katowice 2015

Redaktor serii: Nauki Polityczne
Mariusz Kolczyński

Recenzent
Michał Chorośnicki

Fotografia na okładce: Mike Seyfang / „Fibre” | www.flickr.com

Redakcja: Katarzyna Wyrwas
Projekt okładki: Kamil Gorlicki
Redakcja techniczna: Barbara Arenhövel
Korekta: Lidia Szumigała
Łamanie: Marek Zagniński

ISSN 0208-6336
ISBN 978-83-8012-357-1
(wersja drukowana)
ISBN 978-83-8012-358-8
(wersja elektroniczna)

Wydawca
Wydawnictwo Uniwersytetu Śląskiego
ul. Bankowa 12B, 40-007 Katowice
www.wydawnictwo.us.edu.pl
e-mail: wydawus@us.edu.pl

Wydanie I. Ark. druk. 30,5. Ark. wyd. 43,5.
Papier offset. kl. III, 90 g. Cena 52 zł (+ VAT)

Druk i oprawa: „TOTEM.COM.PL Sp. z o.o.” Sp.K.
ul. Jacewska 89, 88-100 Inowrocław

Spis treści

Wstęp 7

Rozdział 1
Rewolucja informatyczna 25

1.1. Źródła rewolucji informatycznej 25
1.2. Rewolucja informatyczna na przełomie XX i XXI wieku 44
1.3. Istota i implikacje rewolucji informatycznej 53

Rozdział 2
Cyberprzestrzeń jako źródło nowych wyzwań i zagrożeń dla bezpieczeństwa państw 71

2.1. Definicja cyberprzestrzeni 71
2.2. Właściwości techniczne cyberprzestrzeni 85
2.3. Cechy cyberprzestrzeni jako nowego wymiaru bezpieczeństwa państw . . . 93
2.4. Cyberprzestrzeń jako źródło nowych zagrożeń dla bezpieczeństwa państw . . 103

Rozdział 3
Formy zagrożeń teleinformatycznych dla bezpieczeństwa państw . . 115

3.1. Zagrożenia w cyberprzestrzeni w ujęciu podmiotowym 115
3.2. Metody cyberataków 121
3.3. Główne formy zagrożeń dla bezpieczeństwa teleinformatycznego państw . . 133
3.3.1. Zagrożenia nieustrukturalizowane 138
3.3.1.1. Haking 138
3.3.1.2. Haktywizm 142
3.3.1.3. Haktywizm patriotyczny 146
3.3.1.4. Cyberprzestępczość 150

3.3.2. Zagrożenia ustrukturalizowane 155
3.3.2.1. Cyberterroryzm 155
3.3.2.2. Cyberszpiegostwo 161
3.3.2.3. Operacje zbrojne w cyberprzestrzeni 164
3.4. Cyberwojna 169
3.4.1. Cyberwojna jako przedmiot debaty naukowej 169
3.4.2. Definicja cyberwojny 176

Rozdział 4
Cyberprzestrzeń jako nowy wymiar rywalizacji państw 183

4.1. „Pierwsza cyberwojna" w Estonii 184
4.2. Cyberataki w stosunkach litewsko-rosyjskich 202
4.3. Wojna gruzińsko-rosyjska 211
4.4. Cyberataki w stosunkach na linii Rosja — Kirgistan 228
4.5. Operacja *Orchard* 237
4.6. Cyberterroryzm w relacjach Izrael — USA — Iran. *Stuxnet*, *Duqu* i *Flame*. . 250
4.7. Przestrzeń teleinformatyczna jako nowa domena rywalizacji na Półwyspie Koreańskim 275
4.8. Cyberwojna w stosunkach amerykańsko-chińskich 297

Rozdział 5
Cyberprzestrzeń jako nowy wymiar współpracy państw 333

5.1. Organizacja Narodów Zjednoczonych wobec wyzwań dla bezpieczeństwa teleinformatycznego 334
5.2. Cyberzagrożenia w pracach Międzynarodowego Związku Telekomunikacyjnego 351
5.3. Polityka cyberbezpieczeństwa Sojuszu Północnoatlantyckiego 365
5.4. Bezpieczeństwo teleinformatyczne w pracach Unii Europejskiej 378
5.5. Rada Europy wobec zjawiska cyberprzestępczości 394
5.6. Szanghajska Organizacja Współpracy jako narzędzie polityki cyberbezpieczeństwa Chin i Rosji 400
5.7. Polityka bezpieczeństwa teleinformatycznego Współpracy Gospodarczej Azji i Pacyfiku (APEC) 405
5.8. Inicjatywy Organizacji Współpracy Gospodarczej i Rozwoju w dziedzinie cyberbezpieczeństwa 410
5.9. Unia Afrykańska wobec zagrożeń dla bezpieczeństwa teleinformatycznego . . 415

Zakończenie 419

Bibliografia 429

Indeks 475

Summary 485
Résumé 487

Wstęp

Bezprecedensowy rozwój naukowo-techniczny, który rozpoczął się po drugiej wojnie światowej, w ciągu kilku dekad doprowadził do rewolucyjnych zmian we wszystkich sferach życia człowieka. Począwszy od komunikacji, przez rozrywkę, życie społeczne i gospodarcze, aż po procesy polityczne, nowe technologie informacyjne i komunikacyjne, zgodnie z przewidywaniami części deterministów technologicznych (zob. Bimber, 1994), w niespotykany dotychczas sposób zmieniły oblicze świata. Pojawienie się komputerów oraz Internetu, a także innych urządzeń i usług korzystających z dorobku szeroko pojętej teleinformatyki doprowadziło na przełomie XX i XXI wieku do sytuacji, w której ludzkość stała się od nich *de facto* uzależniona. O skali tego zjawiska świadczył fakt, iż w ciągu ostatnich pięciu lat liczba użytkowników Internetu uległa podwojeniu i w 2013 roku wyniosła ok. 2,749 miliarda osób. Oznacza to, że niemal 40% ludzkości regularnie czerpało z potencjału globalnej sieci komputerowej (*Key indicators*, 2013). Jest ona powszechnie używana na masową skalę nie tylko przez pojedynczych użytkowników, ale także przez podmioty sektora prywatnego i publicznego. Z jej możliwości korzystają bowiem organizacje rządowe i pozarządowe, przedsiębiorstwa, korporacje transnarodowe, instytucje administracji publicznej, a nawet siły zbrojne. Nowe technologie na początku XXI wieku stały się więc instrumentem wykorzystywanym powszechnie we wszelkich możliwych wymiarach i płaszczyznach funkcjonowania państw i społeczeństw.

Niespotykany wcześniej w historii ludzkości postęp naukowo-techniczny nie wiąże się jednak wyłącznie z samymi korzyściami. Środowisko naukowe, przede wszystkim w państwach zachodnich, jeszcze w okresie głębokiej zimnej wojny zauważyło, iż rewolucja informatyczna będzie prowadzić do powstawania nowych wyzwań, zarówno w wymiarze politycznym, społecznym, gospodarczym, kulturowym, jak i *stricte* wojskowym. Równolegle temat ten stał się

niezwykle popularny w literaturze fantastyczno-naukowej, która w wielu wypadkach skupiła się na próbach przewidzenia negatywnych konsekwencji pojawienia się nowych technologii. W dyskusji naukowej, która rozgorzała na dobre niemal trzy dekady temu, upowszechniły się jednak głosy i postawy często skrajne, przeceniające wagę problemów w tym zakresie lub niedoceniające jej. Zdaniem części badaczy skala negatywnych następstw rewolucji informatycznej stała się tak duża, iż pojawiło się ryzyko wystąpienia swoistego „cyberarmageddonu", określanego także mianem „elektronicznego Pearl Harbor" lub „elektronicznego Waterloo" (zob. np. Guisnel, 2002: 53; Adams, 2001; Cordesman, Cordesman, 2001: 2; Krepinevich, 2012: 2; Eriksson, Giacomello, 2006: 226). Scenariusz ten zakłada możliwość dokonania strategicznego uderzenia w szeroko rozumianej cyberprzestrzeni, które doprowadziłoby do paraliżu krytycznej infrastruktury państw (zob. Lucky, 2010: 25; Heinl, 2012; Lewis, 2006), przesiąkniętej współcześnie urządzeniami opartymi na ICT (ang. *Information and Communication Technology*)[1]. W literaturze specjalistycznej częstokroć wskazuje się na rosnące zagrożenia dla funkcjonowania sieci elektroenergetycznych, sektora finansowego bądź systemu obronnego, co mogłoby skutkować m.in. odcięciem dostaw energii elektrycznej w skali całego kraju, kryzysem gospodarczym bądź utratą zdolności prowadzenia działań wojennych. Daniel T. Kuehl pisał w tym kontekście, iż Stany Zjednoczone mogą zostać pokonane nawet w ciągu „pierwszej nanosekundy" kolejnego konfliktu zbrojnego. Można tu także wspomnieć o artykule naukowym opublikowanym w 1997 roku, który autorzy zatytułowali wymownie: *Terroryzm informacyjny: Czy możesz zaufać swojemu tosterowi?* (Devost, Houghton, Pollard, 1997: 63—78). Tego typu katastroficzne wizje jak na razie się nie potwierdziły, co bywa podkreślane przez inną grupę ekspertów. Ci z kolei twierdzą, iż problemy na tym tle są często mocno przejaskrawione, a skala wyzwań dla bezpieczeństwa narodowego i międzynarodowego jest w rzeczywistości stosunkowo niewielka (zob. Weimann, 2005; Gartzke, 2013: 41—73).

Wraz z rozprzestrzenianiem się globalnej tkanki systemów teleinformatycznych pojawia się jednak coraz więcej praktycznych przykładów szkodliwego wykorzystania technologii ICT. Pierwsze incydenty tego typu miały miejsce jeszcze w czasie zimnej wojny, choć rozpowszechniły się na masową skalę dopiero na przełomie XX i XXI wieku, wraz z postępem procesów komputeryzacji i informatyzacji[2]. Początkowo były one związane z działalnością

[1] Termin ten wykorzystywany jest od niedawna, przyjął się jednak jako najpełniejsze ujęcie związku pomiędzy rozwiązaniami telekomunikacyjnymi a informatycznymi. W Polsce ICT utożsamia się z reguły z teleinformatyką.

[2] Komputeryzacja polega na zastępowaniu tradycyjnych metod funkcjonowania urzędów państwowych systemami komputerowymi, m.in. przez wprowadzanie elektronicznych baz danych, formularzy internetowych czy listów e-mail jako podstawowych metod komunikacji. Informatyzacja natomiast polega na wykorzystaniu systemów informatycznych do analizy i przetwarzania wprowadzonych danych. Zob. Lakomy, 2011a: 141.

raczej niegroźnego środowiska pasjonatów informatyki, z którego wywodzili się pierwsi hakerzy. Z czasem komputery oraz ich sieci zaczęły być jednak wykorzystywane przez cyberprzestępców, widzących w nich szansę na uzyskanie określonych korzyści osobistych. Równolegle technologie informacyjne i komunikacyjne zyskiwały coraz wyraźniejsze znaczenie polityczne, związane z wyodrębnieniem pierwszych grup haktywistów. Problemy z tym związane, mimo znacznej popularności w mediach (zob. Wall, 2007: 10—15) i kulturze masowej, przez wiele lat nie spotkały się ze zwiększonym zainteresowaniem społeczności międzynarodowej. Rządy poszczególnych państw, z wyjątkiem kilku pionierów w tej dziedzinie, nie dostrzegały szybko rosnącej skali wyzwań. Do przełomu w tym zakresie doszło dopiero w kwietniu i maju 2007 roku, kiedy Estonia jako pierwszy kraj na świecie została zaatakowana przez Internet w niespotykanym wcześniej stopniu. W wyniku trwającej trzy tygodnie kampanii cyberataków nie tylko zablokowano strony internetowe wielu instytucji publicznych, ale także naruszono wybrane elementy infrastruktury krytycznej (Miller, Kuehl, 2009). Jeszcze w tym samym roku we wrześniu Izrael udowodnił, iż cyberprzestrzeń zaczęła się stawać piątym teatrem wojny, obok lądu, morza, przestrzeni powietrznej i kosmicznej. W ramach operacji *Orchard* przeciwko Syrii dokonano sabotażu jej systemu obrony przeciwlotniczej, prawdopodobnie za pomocą włamania komputerowego. W kolejnych latach w sieci doszło do całej gamy innych bardzo poważnych incydentów, które potwierdzały skalę problemów wynikających z niewłaściwego zastosowania osiągnięć rewolucji informatycznej. Przykładowo w sierpniu 2008 roku towarzyszyły one konfliktowi zbrojnemu na Kaukazie. Na przełomie pierwszej i drugiej dekady XXI wieku potencjał nowych technologii został wykorzystany przeciwko Kirgistanowi oraz Iranowi. W tym ostatnim przypadku izraelskie i amerykańskie służby wywiadowcze zastosowały niezwykle zaawansowany, złośliwy program komputerowy *Stuxnet*, aby sabotować program atomowy reżimu ajatollahów. W podobnej sytuacji znalazły się również same Stany Zjednoczone, które stały się najpopularniejszym obiektem miliardów prób włamań komputerowych w ostatnich latach. Cyberataki posłużyły ponadto jako nowy sposób wywierania nacisku politycznego podczas napięć na Półwyspie Koreańskim, między innymi w latach 2011 i 2013.

Pojawia się więc pytanie, jak należy interpretować tego typu wydarzenia oraz jakie jest ich znaczenie dla rozmaitych obszarów życia człowieka i zbiorowości ludzkich. Badania w tym zakresie prowadzi się z wielu rozmaitych perspektyw badawczych. Nauki ścisłe i techniczne skupiają się m.in. na takich kwestiach, jak zabezpieczenia komputerowe, funkcjonalność infrastruktury teleinformatycznej czy nowe technologie telekomunikacyjne. Od lat sfera ta budzi także rosnące zainteresowanie przedstawicieli nauk społecznych, którzy dostrzegają coraz wyraźniejszy związek między postępem naukowo-technicznym a procesami politycznymi, gospodarczymi czy kulturowymi. Jednym z najważ-

niejszych punktów przecięcia badań z obu tych perspektyw jest znaczenie incydentów komputerowych dla bezpieczeństwa narodowego i międzynarodowego. W burzliwej dyskusji poświęconej tym zagadnieniom powstało wiele nowych, wcześniej nieznanych kategorii naukowych, takich jak *cyberterroryzm* lub *cyberwojna*. W zamyśle ich twórców mają one oddawać sens nowych zagrożeń, wynikających z proliferacji technologii teleinformatycznych. Próżno jednak szukać zgody środowiska ekspertów co do jednoznacznego rozumienia tych terminów, a szerzej: co do stosowanej siatki pojęciowej. Nawet w sprawach, które wydawałyby się z pozoru oczywiste, trudno o konsensus, niełatwo bowiem doszukać się podzielanych powszechnie konkluzji co do skali tych wyzwań czy ich bezpośrednich skutków np. dla współczesnej formy konfliktów zbrojnych. Należy się więc zgodzić ze słowami Myriam Dunn-Cavelty (2008: 14), która stwierdziła, iż terminologia ery informacyjnej jest „nieprecyzyjna, dwuznaczna i nieuchwytna".

Jedną z najbardziej kontrowersyjnych kwestii w tej debacie jest rosnąca rola cyberprzestrzeni w stosunkach międzynarodowych. Z pozoru jest to konstatacja naturalna, po bliższym przyjrzeniu okazuje się jednak, iż brak jest pogłębionych analiz, które przy wykorzystaniu narzędzi badawczych właściwych nauce o stosunkach międzynarodowych podjęłyby się sprawdzenia, w jaki sposób ich uczestnicy czerpią z potencjału sieci oraz z jakimi wiąże się to konsekwencjami. Badacze z reguły skupiają się tu na wycinkowych problemach, co utrudnia sformułowanie jednoznacznych wniosków na temat trendów i procesów o zasięgu globalnym. Zdecydowanie bogatsza dyskusja, jak wspomniano, dotyczy zagrożeń teleinformatycznych i ich znaczenia dla bezpieczeństwa narodowego i międzynarodowego, niewiele jest natomiast analiz, które wpisywałyby te zagadnienia w szersze ramy działań poszczególnych podmiotów funkcjonujących w środowisku międzynarodowym. Praca ta jest więc reakcją na tę konstatację. Dostrzegając kolejne incydenty komputerowe, które w coraz większym stopniu zagrażają bezpieczeństwu państw, warto zadać pytanie, czy cyberprzestrzeń nie staje się nową sferą ich naturalnej rywalizacji. To samo tyczy się drugiego oczywistego aspektu ich aktywności zewnętrznej, czyli współpracy. Charakterystyka tego zagadnienia nie może się jednak oprzeć jedynie na prostym przeglądzie empirycznych przykładów tzw. cyberwojen, powinna natomiast ująć je zdecydowanie szerzej, w kontekście całokształtu zachowań podmiotów w środowisku międzynarodowym.

Główna hipoteza monografii zawiera się w stwierdzeniu, iż cyberprzestrzeń stała się nowym wymiarem polityki zagranicznej. Państwa w XXI wieku coraz częściej wykorzystują cyberataki, aby realizować swoje interesy w środowisku międzynarodowym, co implikuje zjawisko ich rywalizacji w przestrzeni teleinformatycznej. Ze względu na jej właściwości techniczne, otwartą architekturę, potencjał dla szeroko pojętej sfery informacyjnej czy brak obowiązujących regulacji prawno-politycznych, środki te jawią się jako dogodna i coraz skutecz-

niejsza metoda osiągania celów na arenie międzynarodowej. Rodzi to jednak zarazem poważne zagrożenia dla bezpieczeństwa państw, a szerzej: dla całego systemu międzynarodowego. Warunkuje to zatem również proces wzrastającej współpracy państw w zakresie bezpieczeństwa teleinformatycznego.

Na tej podstawie wysunięto następujące hipotezy robocze:

1. Rewolucja informatyczna oprócz niezaprzeczalnych korzyści przyniosła nowe zagrożenia dla bezpieczeństwa państw.
2. Cyberprzestrzeń ze względu na swoje unikalne właściwości stała się wymiarem, w którego ramach można stosować rozmaite instrumenty polityki zagranicznej.
3. Do najczęściej używanych środków należą: cyberterroryzm, cyberszpiegostwo oraz operacje zbrojne w cyberprzestrzeni. Unikalną rolę odgrywa także haktywizm patriotyczny, będący swoistym *quasi*-instrumentem.
4. Wykorzystanie cyberprzestrzeni przez państwa otwiera nowe możliwości realizowania interesów na arenie międzynarodowej. „Teleinformatyczne" instrumenty polityki zagranicznej pozwalają w niestandardowy sposób osiągać takie cele, jak zapewnienie bezpieczeństwa, wzrost potęgi (siły) oraz wzrost pozycji i prestiżu międzynarodowego. Ich skuteczność bywa jednak różna i mają one z reguły charakter komplementarny w stosunku do innych środków.
5. Ich zastosowanie przez poszczególne rządy determinuje zjawisko rywalizacji państw w cyberprzestrzeni.
6. Środki te stanowią zarazem nowy rodzaj zagrożeń dla bezpieczeństwa narodowego i międzynarodowego, są zatem również czynnikiem sprzyjającym zawiązywaniu współpracy państw w dziedzinie bezpieczeństwa teleinformatycznego.
7. Mimo że zakres kooperacji w cyberprzestrzeni w ostatnich latach stopniowo rośnie, nadal nie wypracowano w tej dziedzinie najpotrzebniejszych mechanizmów i rozwiązań.
8. W XXI wieku można odnotować przewagę rywalizacyjnej aktywności państw w cyberprzestrzeni nad aspektami koncyliacji i współpracy, co wiąże się z poważnymi konsekwencjami dla systemu międzynarodowego. Można tu wskazać na dwa najistotniejsze skutki: osłabienie efektywności prawa międzynarodowego oraz osłabienie skuteczności mechanizmów współpracy politycznej i wojskowej.

Głównym celem naukowym monografii jest więc wyjaśnienie, czy państwa rywalizują i współpracują w cyberprzestrzeni, czym się to przejawia oraz jakie są tego konsekwencje dla praktyki polityki zagranicznej oraz całokształtu stosunków międzynarodowych. Innymi słowy opracowanie to stara się odpowiedzieć na pytanie, czy działania w przestrzeni teleinformatycznej mogą być uznane za instrument polityki zagranicznej, zarówno w ujęciu rywalizacyjnym, jak i kooperacyjnym. Tego typu praktyka wiązałaby się bowiem z zasadniczymi

skutkami dla całego systemu międzynarodowego, nie tylko z perspektywy bezpieczeństwa.

Celem pracy jest również odpowiedź na szereg pytań badawczych, które powinny ułatwić realizację celu głównego:

1. Jakie były najważniejsze procesy i wydarzenia determinujące rewolucję informatyczną w XX i XXI wieku oraz jej podstawowe reperkusje dla funkcjonowania państw i społeczeństw?
2. Czym jest cyberprzestrzeń oraz jakie posiada właściwości z punktu widzenia jej przydatności dla czynników państwowych?
3. Czym są cyberataki oraz jakie są ich podstawowe metody w ujęciu technicznym?
4. Jakie są najpoważniejsze formy zagrożeń teleinformatycznych dla bezpieczeństwa państw z perspektywy nauki o stosunkach międzynarodowych?
5. Czy cyberataki można uznać za świadomy środek realizowania interesów państwa na arenie międzynarodowej? Jeśli tak, to jakie cele są w ten sposób realizowane oraz jaka jest ich skuteczność w porównaniu do zakładanych oczekiwań?
6. Czy rosnąca skala incydentów teleinformatycznych doprowadziła do nawiązania międzynarodowej współpracy w zakresie cyberbezpieczeństwa? Jeśli tak, to w jaki sposób się to przejawia oraz jaka jest skuteczność tej współpracy?
7. Jaki jest wpływ rywalizacji i współpracy państw w cyberprzestrzeni na bezpieczeństwo międzynarodowe?
8. Jaki jest wpływ rywalizacji i współpracy państw w cyberprzestrzeni na praktykę polityki zagranicznej?
9. Jaki jest wpływ rywalizacji i współpracy państw w cyberprzestrzeni na skuteczność prawa międzynarodowego i mechanizmów współpracy politycznej?

Aby zrealizować postawiony wyżej cel, odpowiedzieć na pytania badawcze oraz dokonać weryfikacji hipotezy głównej i hipotez roboczych, należałoby na wstępie wyjaśnić kilka kwestii. Przede wszystkim, o czym wspomniano już wyżej, problematyka szeroko pojętych konsekwencji szkodliwego wykorzystania technologii teleinformatycznych jest podejmowana nie tylko przez nauki społeczne, lecz również przez nauki techniczne i ścisłe. Podchodzą one do tych zagadnień odmiennie, co może czasami rodzić poważne spory terminologiczne i interpretacyjne. Każda z dziedzin wykształciła aparat pojęciowy (nie zawsze zresztą podzielany przez całe środowisko naukowe), skupiający się na właściwych jej zagadnieniach, który niekoniecznie musi być przydatny do analizy podobnych spraw z perspektywy innego obszaru wiedzy. W monografii zatem, bazując naturalnie na dotychczasowym dorobku nauk technicznych i ścisłych, podjęto badania z perspektywy stosunków międzynarodowych. Ma to określone konsekwencje dla stosowanych metod badawczych. Takie dyscypliny naukowe,

jak informatyka czy elektronika, operują z reguły bardzo konkretnymi, wyraźnie sprecyzowanymi kategoriami i pojęciami naukowymi. W ujęciu społecznym, na różnych poziomach analizy, tak z reguły nie jest. Na styku nowych technologii oraz czynnika ludzkiego, szczególnie w wymiarze politycznym i bezpieczeństwa, pojawiają się bowiem zjawiska dynamiczne, bardzo trudne do jednoznacznej oceny. Częstokroć poszczególne sposoby wykorzystania ICT nawzajem się przenikają i mają skutki na wielu pozornie niezwiązanych ze sobą płaszczyznach. Rodzi to oczywiste problemy dla metodologii badań nad aktywnością państw w cyberprzestrzeni. Jak bowiem wspomniano wcześniej, nie ma szeroko podzielanego konsensusu przedstawicieli nauk o polityce, nauk o bezpieczeństwie czy nauk o obronności co do stosowanej w tym zakresie siatki pojęciowej. W konsekwencji w literaturze specjalistycznej częstokroć używa się bardzo zróżnicowanej, a niekiedy mało sprecyzowanej nomenklatury naukowej. W związku z tym warunkiem *sine qua non* dokonania analizy rywalizacji i współpracy państw w cyberprzestrzeni powinno być zaproponowanie odpowiadającej stanowi faktycznemu terminologii w tym zakresie.

Ponadto powstaje pytanie, na jakim poziomie należałoby rozpatrywać postawiony problem badawczy. Jak pisał Edward Haliżak (2013a: 28), „wybór danego poziomu analizy wiąże się zawsze z przyjęciem określonych założeń ontologicznych" oraz „pełni ważną funkcję eksplanacyjną". W tym kontekście najbardziej właściwy wydaje się poziom polityki zagranicznej, rywalizację i współpracę państw w różnych wymiarach i płaszczyznach można bowiem uznać za konsekwencję realizacji odmiennych lub zbieżnych interesów i celów ich aktywności zewnętrznej. Odwołując się do rozważań Wojciecha Kosteckiego, wzięto pod uwagę dwa poziomy analizy polityki zagranicznej: państwowy oraz międzynarodowy. W pierwszym przypadku politykę zagraniczną „traktuje się jako rezultat krajowego splotu określonych czynników", w drugim natomiast „interpretowana jest jako reakcja na środowisko zewnętrzne" (Kostecki, 2012: 119), przy czym należy stwierdzić, że przyjęcie takiej optyki badawczej sprawia, iż formułowane wnioski dotyczą również wyższego poziomu — całego systemu międzynarodowego.

Analizując rywalizację i współpracę państw w nowej domenie, jaką jest cyberprzestrzeń, należałoby już na wstępie przyjąć określone definicje podstawowych terminów i kategorii z zakresu teorii polityki zagranicznej, które posłużą do rozważań w dalszych częściach pracy. Ze względu na fakt, iż kwestie te zostały już bardzo szeroko i wyczerpująco omówione w polskiej i zagranicznej literaturze specjalistycznej[3], nie ma sensu omawiać ich osobno w pierw-

[3] Zob. np.: Kukułka, 2003; Nowiak, 2000; Zięba, 2005a,b; Łoś-Nowak, 2008; Kostecki, 1988; Łoś-Nowak, 2011; Cziomer, 2005; Dobroczyński, Stefanowicz, 1984; Malendowski, Mojsiewicz, Czachór, Bryła, 2007; Holsti, 1967; Kondrakiewicz, 2013; Ociepka, 2013; Zając, 2005; Popiuk-Rysińska,1992; Bryła, 2000.

szym rozdziale pracy[4]. Przyjęto więc rozumienie polityki zagranicznej za Teresą Łoś-Nowak (2011: 47), która zauważyła, iż jest to „dynamiczny proces formułowania i realizacji interesów narodowych i celów polityki w poliarchicznym i policentrycznym środowisku międzynarodowym". Jeśli chodzi o cele polityki zagranicznej, kategorię o fundamentalnym znaczeniu dla realizacji celu badawczego, zdecydowano się na przyjęcie ich podziału za Ryszardem Zięba (2005a: 48—49), który wyróżnił cztery grupy celów: zapewnienie bezpieczeństwa państwa w stosunkach międzynarodowych, wzrost siły państwa, wzrost pozycji międzynarodowej i prestiżu oraz kształtowanie i optymalizacja reguł funkcjonowania środowiska międzynarodowego. Jeśli chodzi o pierwszą grupę celów, najpełniej oddał jej charakter Marian Dobrosielski (cyt. za: Malendowski, 2000: 386):

> przez zagwarantowanie bezpieczeństwa danego państwa rozumiemy dziś tworzenie takich warunków, które zapewniałyby mu istnienie własnej państwowości, suwerenności, integralność terytorialną, nieingerencję w sprawy wewnętrzne. Warunków, które umożliwiłyby rozwój osobowości i tożsamości narodowej, własnego języka, gospodarki, nauki i innych dziedzin życia. Chodzi więc o kształtowanie takiej sytuacji, która mogłaby zapewnić realizację celów, wartości, aspiracji danego państwa czy społeczeństwa, jego trwałych, żywotnych interesów.

Wzrost potęgi i siły Erhard Cziomer (2005: 131) określił jako wykorzystanie „wszelkich atutów wewnętrznych dla osiągania korzystnych efektów w kontaktach politycznych, gospodarczych, społecznych itp. z innymi państwami oraz uczestnikami stosunków międzynarodowych". Trzecia grupa celów zdaniem Ryszarda Zięby (2005a: 54) wyraża „koegzystencjalne interesy wyrastające z potrzeb: uczestnictwa w systemie międzynarodowym […], współpracy i współzawodnictwa z innymi państwami i narodami, potwierdzania suwerenności państwa i wzrostu jego roli międzynarodowej". Czwarta grupa celów polityki zagranicznej wywodzi się natomiast z wartości uniwersalnych, nie opiera się na egoizmie i dotyczy m.in. wsparcia międzynarodowego pokoju, umacniania systemu międzynarodowego, przeciwdziałania zagrożeniom dla bezpieczeństwa oraz rozwoju prawa i zwyczajów międzynarodowych (Ibidem, s. 56—68). W literaturze przedmiotu oprócz celów wyróżnia się jeszcze środki polityki zagranicznej, przez które można rozumieć „wszystkie zasoby i instrumenty, przy użyciu których państwa starają się kształtować pożądane postawy

[4] W pierwotnej wersji tej rozprawy pierwszy rozdział nosił tytuł *Pojęcie, uwarunkowania, cele i środki polityki zagranicznej.* Szeroko charakteryzował on dotychczasową dyskusję na ten temat, uwzględniając również wątki związane z rozumieniem rozmaitych kategorii związanych z bezpieczeństwem. Ze względu jednak na słuszną uwagę Recenzenta, iż sprawy te zostały już wielokrotnie omówione w literaturze specjalistycznej, zdecydowano się na jego usunięcie.

i działania zagranicznych podmiotów oraz pożądane stany zjawisk i procesów międzynarodowych”[5].

Na tym tle, należałoby również wyjaśnić, czym jest rywalizacja i współpraca państw. W pracy przyjęto rozumienie rywalizacji za Agatą Włodowską-Bagan (2012: 105, 111)[6], według której

> Dokonując pewnego uogólnienia, można […] wskazać dwa elementy, które wydają się niezbędne dla uznania stosunków między państwami za rywalizację. Po pierwsze, chodzi o […] sprzeczność interesów, wynikającą z jednoczesnego ubiegania się o pierwszeństwo lub zdobycie czegoś lub kogoś, a po drugie o czynnik psychologiczny związany z identyfikacją państwa jako rywala. […] Należy dokonać tu wyraźnego rozróżnienia, jako że nie każdy konflikt jest rywalizacją i nie w każdej rywalizacji mamy do czynienia z użyciem siły. Rywalizacja, choć może być przyczyną konfliktów, nie jest jednak niezbędna do ich powstawania.

Z kolei współpracę państw trafnie wyjaśnił Robert Koehan, który stwierdził, iż „ma [ona — M.L.] miejsce wtedy, gdy uczestnicy dostosowują swoje zachowanie do aktualnych i oczekiwanych preferencji innych uczestników poprzez proces koordynacji działań” (cyt. za: Haliżak, 2006: 236).

Oprócz podstawowych pojęć i klasyfikacji z zakresu teorii polityki zagranicznej ze względu na podejmowaną w rozprawie problematykę należałoby we wstępie także wyjaśnić, co rozumie się przez bardzo pojemny termin, jakim jest *bezpieczeństwo*[7]. Definicję bezpieczeństwa narodowego przyjęto zatem za Waldemarem Kitlerem (2002: 48), który rozumiał przez to proces obejmujący zabiegi (np. politykę zagraniczną, przedsięwzięcia ochronne i obronne), których celem jest stworzenie korzystnych warunków funkcjonowania państwa na „arenie międzynarodowej oraz wewnętrznej oraz przeciwstawienie się wyzwaniom i zagrożeniom bezpieczeństwa”. Z kolei bezpieczeństwo międzynarodowe zgodnie z interpretacją Romana Kuźniara (2012a: 15) uznano za „brak zagrożeń dla norm, reguł i instytucji, które służą zapewnianiu bezpieczeństwa państw i pozostałych uczestników stosunków międzynarodowych”. Należy przy tym zaznaczyć, że oba te pojęcia są uznawane obecnie za nieostre, co wynika m.in. z coraz

[5] Rozróżnia się środki polityczne, ekonomiczne, wojskowe, kulturowo-ideologiczne oraz inne. Oprócz nich funkcjonuje pojęcie metod polityki zagranicznej, przez które Justyna Zając (2005: 79—80) rozumie „sposoby posługiwania się przez państwa środkami. Metody te można podzielić na: pozytywne, czyli nakłanianie; negatywne, czyli przymus, oraz neutralne”.

[6] Zob. także Sułek, 2012: 35—49.

[7] Zob. np.: Kowalkowski, 2011; Zięba, 2011; Czaputowicz, 2006, 2012; Kołodziej, 1997; Pietraś, 2000; Kuźniar, 2006a,b; Kukułka, 1995; Baldwin, 1997; Bobrow, 1997; Cziomer, 2005; Kuźniar, Balcerowicz, Bieńczyk-Missala, Grzebyk, Madej, Pronińska, Sułek, Tabor, Wojciuk, 2012; Wolfers, 1952; Kuźniar, 2012a,b; Herz, 1959; Madej, 2005; Kitler, 2002; Gała, 2009; Łebkowska, 2011; Mojsiewicz, 2000.

szerszej gamy determinantów wpływających w okresie pozimnowojennym na bezpieczeństwo państw. Jak stwierdził Marek Madej (2005: 491):

> stopniowo krystalizuje się współczesne pojmowanie bezpieczeństwa, bardziej systemowe, całościowe i wszechstronne (tzn. obejmujące możliwie najpełniejsze spektrum zagadnień i sfer życia społecznego, na których mogą powstawać problemy bezpieczeństwa). Takie ujęcie (czy też ujęcia, nie można bowiem w tym przypadku mówić o jednym, dominującym modelu) lepiej odpowiada obecnemu kształtowi stosunków międzynarodowych, w których relacje między poszczególnymi ich uczestnikami dalece odbiegają […] od względnej jednoznaczności okresu zimnowojennego.

W związku z tym w ujęciu przedmiotowym (Kukułka, 1994: 40—41) wyróżnia się już nie tylko bezpieczeństwo polityczne (Pawlikowska, 2005: 62) i wojskowe (Balcerowicz, 2005: 478—481; Nowak, Nowak, 2011: 72; Żukrowska, 2006: 32), lecz także gospodarcze (ekonomiczne) (Haliżak, 1997: 78; Anokhin, Grishin, 2013: 155—163), ekologiczne (Pietraś, 2000: 20) czy społeczno-kulturowe (Czaputowicz, 2006: 75; Leszczyński, 2011; Michałowska, 1997; Lizak, 1997; Zakrzewski S., 2013: 165—174).

Od pewnego czasu coraz częściej dodaje się do tej listy jeszcze jeden, kluczowy dla dalszych rozważań, wymiar przedmiotowy bezpieczeństwa. Jak pisali Agnieszka Bógdał-Brzezińska i Marcin Florian Gawrycki (2003: 40—41):

> wraz z postępem technologicznym i cywilizacyjnym sfera bezpieczeństwa publicznego rozszerzyła się na nowe dziedziny. Współczesne pojęcie bezpieczeństwa informacyjnego lub cybernetycznego (*cybersecurity*) odnosi się zatem do stosunkowo młodej, ale bardzo prężnie rozwijającej się i bardzo wrażliwej sfery ICT. Jest ona zarówno obszarem prywatnej aktywności obywateli, jak też strategicznym czynnikiem rozwoju gospodarki narodowej (cyberekonomia).

W związku z tym, zdaniem autorów, „bezpieczeństwo informacyjne (BI) funkcjonuje w powiązaniu z szeregiem tradycyjnych wymiarów bezpieczeństwa państwa" (Ibidem). W tym kontekście część badaczy, omawiając te zagadnienia, pisze o bezpieczeństwie informacyjnym rozumianym często jako „ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania" (Liedel, 2011: 56—57). W literaturze specjalistycznej przyjmuje się jednak często inne podejście, zakładające skupienie się wyłącznie na problematyce związanej z technologiami teleinformatycznymi[8], a nie szerszą kategorią infor-

[8] Józef Janczak oraz Andrzej Nowak (2013: 20—21) stwierdzili, że bezpieczeństwo informacyjne jest pojęciem bardzo szerokim i można je podzielić na dwa rodzaje: bezpieczeństwo informacji (ochrona wszystkich form wymiany, przechowywania i przetwarzania danych) oraz bezpieczeństwo teleinformatyczne.

macji[9]. Wobec tego ujęcie to określa się z reguły mianem *bezpieczeństwa teleinformatycznego* lub *cyberbezpieczeństwa*. Można przez to rozumieć za Markiem Madejem i Marcinem Terlikowskim (2009: 10—11)

> zdolność określonego podmiotu do pozyskania i zachowania, w formie niezmienionej bez jego zgody i wiedzy, wszelkiego rodzaju informacji utrwalonej w postaci cyfrowej oraz możliwość jej bezpiecznego (tzn. nienarażonego na przechwycenie, zniszczenie lub nieuprawnioną modyfikację) przetwarzania, przesyłania i upowszechniania[10].

Znając znaczenie podstawowych terminów wykorzystywanych w dalszych częściach pracy, warto odnieść się wreszcie do pewnych wątpliwości związanych z dostępnością faktografii. Analiza aktywności państw w cyberprzestrzeni rodzi bowiem zasadnicze trudności, wynikające z obiektywnych właściwości tej domeny. Jej charakter sprawia, iż jednoznaczna identyfikacja pośrednich i bezpośrednich sprawców cyberataków bywa bardzo trudnym, a czasami wręcz niemożliwym zadaniem. W przeciwieństwie do badań skupiających się na wydarzeniach politycznych, gospodarczych czy wojskowych ustalenie faktów związanych z działaniami w sieciach komputerowych jest o wiele bardziej skomplikowane. W związku z tym przyjęto tu kilka rozwiązań. Przede wszystkim bez względu na fakt, iż jest to praca z dziedziny nauk społecznych, oparto się bardzo szeroko na analizach przeprowadzonych przez przedstawicieli nauk ścisłych i technicznych. Szczególnie przydatne do omówienia przypadków rywalizacji państw w przestrzeni teleinformatycznej okazały się opracowania czołowych korporacji zajmujących się zabezpieczeniami komputerowymi czy zwalczaniem złośliwego oprogramowania (np. Symantec, McAfee czy Kaspersky Lab). Bardzo często w toku prowadzonych przez nie badań natrafiano na wskazówki lub dowody pozwalające na identyfikację osób bądź podmiotów odpowiedzialnych za dane włamanie. Podobne osiągnięcia odnotowało wiele zespołów naukowców lub ośrodków analizujących zagrożenia dla bezpieczeństwa teleinformatycznego, takich jak np.

[9] Krzysztof Liedel (2011: 56—57) zauważył, iż informacja stanowi w XXI wieku zasób strategiczny, wynikająca z niej wiedza i technologie stają się podstawowym czynnikiem wytwórczym, dochody państwa w coraz większym stopniu będą uzyskiwane dzięki sektorowi informacyjnemu, procesy decyzyjne w innych sektorach gospodarki i życia społecznego będą uzależnione od systemów przetwarzania i przesyłania informacji, ich zakłócenie nie wymaga wielkich nakładów, a rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej. Z kolei Krzysztof Liderman (2009: 10) uznał, że informacja „była, jest i będzie towarem. Informacje mają jednak tę szczególną właściwość, odróżniającą je od innych towarów (przedmiotów materialnych, usług), że aby udzielić ich jednym (osobom), wcale nie trzeba odbierać ich innym".

[10] W tym kontekście mówi się też często o swoistej triadzie bezpieczeństwa teleinformatycznego, w której skład wchodzą integralność, poufność oraz dostępność informacji. Zob. Madej, Terlikowski, 2009: 10—11.

kanadyjski Citizen Lab. Na tej podstawie starano się wskazać, czy istniała korelacja między motywami, celami polityki zagranicznej poszczególnych państw a incydentami teleinformatycznymi. Jeśli taki związek istniał, był to kolejny argument pozwalający na przyjęcie określonej interpretacji wydarzeń. Wreszcie sprawdzano, czy ataki komputerowe wpisywały się w specyfikę całokształtu stosunków dwu- lub wielostronnych i jaką odgrywały w nich potencjalnie rolę.

Wszystkie powyższe założenia wymagały więc zastosowania szeregu metod badawczych właściwych dla nauk społecznych. Przede wszystkim wykorzystano metodę analizy historycznej, przydatnej do omówienia przebiegu i globalnych skutków rewolucji informatycznej w XX i XXI wieku. Odpowiedź na pytanie, jak w przeszłości ewoluowały technologie informacyjne i komunikacyjne, miała fundamentalne znaczenie dla zrozumienia fenomenu cyberprzestrzeni jako nowej domeny rywalizacji i współpracy państw. Po drugie — odwołano się do metody analizy treści m.in. oficjalnych dokumentów, wypowiedzi polityków bądź opinii analityków. Jak wspomniano bowiem wyżej, od niemal trzech dekad trwa bardzo ożywiona debata na temat konsekwencji szkodliwego wykorzystania technologii informatycznych. Charakterystyka tych zagadnień bez znajomości najnowszych trendów i wniosków z tej dyskusji nie byłaby więc możliwa. Po trzecie — w rozdziałach dotyczących empirycznych przykładów rywalizacji i współpracy odwołano się do metody analizy decyzyjnej oraz analizy instytucjonalno-prawnej. Metoda decyzyjna pomogła w wyjaśnieniu zjawisk międzynarodowych na podstawie konkretnych decyzji politycznych. Kluczowe było tu wskazanie nie tylko powodów podjęcia danej decyzji, ale także jej wpływu na całokształt rzeczywistości międzynarodowej. Z kolei metoda instytucjonalno-prawna, polegająca na badaniu aktów normatywnych, była szczególnie przydatna przy analizie przejawów współpracy rządów w tej dziedzinie. Po czwarte — zastosowano metodę komparatywną dla porównania, w jaki sposób poszczególne podmioty wykorzystywały potencjał sieci teleinformatycznych do realizacji określonych celów w środowisku międzynarodowym. Po piąte — aby zrozumieć globalny charakter zagrożeń teleinformatycznych oraz ich wpływ na stosunki międzynarodowe, użyto metod ilościowych (statystycznych), polegających na zebraniu i przetworzeniu masowych informacji o niekorzystnych trendach w cyberprzestrzeni. Odwołano się ponadto do kilku podstawowych metod badawczych, takich jak analiza i krytyka źródeł, analiza i krytyka piśmiennictwa, metoda obserwacji faktów oraz synteza i opis*.

Struktura pracy ma charakter problemowy. W rozdziale pierwszym przedstawiono główne etapy, istotę i konsekwencje rewolucji informatycznej. Omówienie tych zagadnień było o tyle ważne, iż stanowiło podstawowy warunek

* W pierwotnej wersji pracy zastosowano przypisy dolne. W procesie wydawniczym, ze względu na znaczną ich liczbę oraz związane z tym wątpliwości co do czytelności monografii, zdecydowano o zastosowaniu zmodyfikowanego systemu harwardzkiego. Jednocześnie ze względu na specyfikę pracy pozostawiono w przypisach dolnych liczne źródła internetowe.

zrozumienia potencjału technologii teleinformatycznych oraz ich wpływu na funkcjonowanie człowieka i jego zbiorowości. W tym kontekście scharakteryzowano główne osiągnięcia i odkrycia poczynione w XX i XXI wieku, zarówno z dziedzinie telekomunikacji, jak i informatyki. Szczególny nacisk położono na proces powstawania sieci komputerowych oraz wynikających z tego implikacji dla najważniejszych obszarów życia ludzkiego, w tym komunikacji, polityki, kultury, gospodarki czy życia społecznego.

Na tej podstawie w rozdziale drugim omówiono, czym jest cyberprzestrzeń[11] oraz z jakimi konsekwencjami wiąże się jej funkcjonowanie. Przede wszystkim scharakteryzowano wieloletnią debatę poświęconą temu pojęciu, konfrontując się zarówno z jego zwolennikami, jak i przeciwnikami. Następnie przyjęto własną interpretację znaczenia tego terminu, co było warunkiem przejścia do dalszych etapów badań. Omówiono ponadto główne właściwości techniczne cyberprzestrzeni, w tym wielowarstwowy, wielopodmiotowy charakter związany z otwartą architekturą czy promieniowaniem elektromagnetycznym. Wskazano również na jej najważniejsze cechy jako nowego wymiaru bezpieczeństwa narodowego i międzynarodowego. Tym samym przedstawiono powody, dla których przestrzeń teleinformatyczna stała się interesującą i unikalną sferą realizacji interesów i celów polityki zagranicznej. Scharakteryzowano także pokrótce ewolucję szkodliwej aktywności w sieciach komputerowych, począwszy od lat 60. XX wieku, współczesną skalę oraz konsekwencje o zasięgu globalnym.

W rozdziale trzecim podjęto próbę sformułowania podstawowej siatki pojęciowej dotyczącej zagrożeń dla bezpieczeństwa teleinformatycznego w oparciu o wcześniejsze rozważania oraz wieloletnią debatę naukową na ten temat. Niezbędna dla zrozumienia aktywności państw w cyberprzestrzeni analiza tych wyzwań wyszła od wskazania głównych podmiotów odpowiedzialnych za szkodliwą działalność w sieci. Wzięto tu pod uwagę dwa czynniki: stopień organizacji sprawców oraz ich motywacje. Zdefiniowano również, czym są cyberataki oraz jakie są ich główne metody w ujęciu technicznym. Na tej podstawie skonstruowano uproszczoną typologię zagrożeń teleinformatycznych, do których zaliczono haking, haktywizm, cyberprzestępczość, haktywizm patriotyczny, cyberszpiegostwo, cyberterroryzm oraz operacje zbrojne w cyberprzestrzeni. Scharakteryzowano ponadto kontrowersyjne zjawisko cyberwojny, odnosząc się zarówno do krytyków, jak i zwolenników stosowania tej kategorii.

Rozdział czwarty został poświęcony analizie empirycznych przykładów rywalizacji państw w cyberprzestrzeni oraz wynikających z tego konsekwencji dla ich bezpieczeństwa oraz polityki zagranicznej. Do analizy wybrano osiem najlepiej udokumentowanych oraz najbardziej znanych przykładów: stosunki na linii Rosja — Estonia, Rosja — Litwa, Rosja — Gruzja, Rosja — Kirgistan,

[11] W pracy używano także synonimów: *przestrzeń teleinformatyczna*, *środowisko teleinformatyczne*.

Izrael — Syria, Izrael — USA — Iran, USA — Chiny oraz Korea Północna — Korea Południowa[12]. W badaniu brano pod uwagę przede wszystkim uwarunkowania stosunków dwu- lub wielostronnych oraz interesy i cele formułowane przez wszystkie zainteresowane strony. Dalej omawiano przebieg i specyfikę incydentów teleinformatycznych oraz ich wpływ na bezpieczeństwo zaatakowanych podmiotów. Na tej podstawie dokonywano próby określenia, czy cyberataki rzeczywiście zostały wykorzystane w charakterze nowego, unikalnego środka polityki zagranicznej. Jeśli odpowiedź była twierdząca, starano się zidentyfikować cele, które w ten sposób realizowano, oraz skuteczność takich przedsięwzięć.

W rozdziale ostatnim przedstawiono natomiast cyberprzestrzeń jako nowy wymiar współpracy państw. Omówiono tu powody, dzięki którym społeczność międzynarodowa w coraz większym stopniu wykazuje chęć kooperacji w tym zakresie. Scharakteryzowano ponadto globalną debatę, która od lat toczy się w łonie Organizacji Narodów Zjednoczonych, m.in. nad zjawiskiem cyberprzestępczości, cyberwojny czy nieskutecznością prawa międzynarodowego. Wskazano także na unikalny *casus* Międzynarodowego Związku Telekomunikacyjnego, będącego organizacją, która wypracowała jak dotąd najskuteczniejsze mechanizmy praktycznej współpracy w tej dziedzinie. Omówiono również najbardziej zaawansowane przedsięwzięcia podejmowane na szczeblu regionalnym na przykładzie Paktu Północnoatlantyckiego oraz Unii Europejskiej oraz przedstawiono aktywność w tej sferze kilku innych organizacji międzynarodowych, takich jak Rada Europy, Unia Afrykańska czy Organizacja Współpracy Gospodarczej i Rozwoju[13]. Na tej podstawie spróbowano odpowiedzieć na pytanie, jaka jest skuteczność tego typu środków w świetle oczekiwanych przez państwa członkowskie rezultatów współpracy na arenie międzynarodowej.

Temat monografii nie doczekał się dotychczas zwartego opracowania w polskiej i zagranicznej literaturze naukowej. Od końca XX wieku coraz częściej pojawiają się ciekawe prace naukowe poświęcone szkodliwemu wykorzystaniu cyberprzestrzeni. Zdecydowana większość publikacji na ten temat zawęża jednak problematykę badawczą wyłącznie do aspektów związanych z bezpie-

[12] Oczywiście nie zamyka to listy wszystkich znanych opinii publicznej incydentów teleinformatycznych, których stronami były państwa. Wybrane przykłady spotkały się jednak z największym zainteresowaniem badaczy oraz były przedmiotem pogłębionych analiz zarówno z perspektywy nauk społecznych, jak i technicznych. Nie podjęto więc w pracy tych wątków, które nie zostały w wyczerpujący sposób omówione przez ekspertów z zakresu informatyki bądź ich znaczenie dla omawianego tematu jest nikłe. Chodzi tu m.in. o takie przypadki, jak rola cyberataków w stosunkach indyjsko-pakistańskich czy izraelsko-palestyńskich.

[13] Klucz doboru oparto na dwóch przesłankach. Po pierwsze: celem było wyeksponowanie dorobku kilku organizacji rządowych mających relatywnie duże znaczenie w systemie stosunków międzynarodowych. Po drugie: zaprezentowano podmioty, które przyjmowały możliwie jak najbardziej zróżnicowane podejście do tematyki cyberbezpieczeństwa, odnosząc w tym wymiarze zarówno sukcesy, jak i ponosząc spektakularne porażki. Pozwoliło to na zobrazowanie szerokiego spektrum przedsięwzięć w tej dziedzinie.

czeństwem teleinformatycznym, zarówno w ujęciu politologicznym, jak i prawnym, technicznym bądź wojskowym. Z reguły bardzo skrótowo podejmuje się natomiast wątki szerszych konsekwencji aktywności państw w sieci na poziomie narodowym i międzynarodowym. Bez względu na ten fakt w pracy wykorzystano bogatą literaturę polsko-, anglo- oraz francuskojęzyczną. Jeśli chodzi o polskie opracowania, to nie sposób wymienić wszystkich autorów, których dzieła pomogły w analizie zjawiska rywalizacji i współpracy państw w cyberprzestrzeni. Warto jednak wymienić tych, których monografie bądź artykuły okazały się najbardziej przydatne: Piotr Sienkiewicz, Marek Madej, Marcin Terlikowski, Marcin Florian Gawrycki, Agnieszka Bógdał-Brzezińska, Krzysztof Liedel, Paulina Piasecka, Krzysztof Liderman oraz Ernest Lichocki. Piotr Sienkiewicz jest uznawany za jeden z największych krajowych autorytetów, jeśli chodzi o takie zagadnienia, jak wojna i walka informacyjna, cyberbezpieczeństwo, a także dowodzenie, cybernetyka czy inżynieria systemów (zob. Goban-Klas, Sienkiewicz, 1999; Sienkiewicz, 2003; Sienkiewicz, Świeboda, 2006, 2009). Marek Madej i Marcin Terlikowski są redaktorami jednej z najciekawszych prac zbiorowych poświęconych bezpieczeństwu teleinformatycznemu państw oraz autorami interesujących publikacji na ten temat (Madej, Terlikowski, red., 2009; Terlikowski, Rękawek, Kozłowski, 2014). Marcin Florian Gawrycki oraz Agnieszka Bógdał-Brzezińska w wielu swoich publikacjach nie tylko wnikliwie scharakteryzowali zjawisko cyberterroryzmu, ale także inne niekorzystne konsekwencje rewolucji informatycznej (Bógdał-Brzezińska, Gawrycki, 2003, 2004; Bógdał-Brzezińska, 2009). Krzysztof Liedel oraz Paulina Piasecka są z kolei uznanymi autorami wielu przydatnych prac z zakresu szeroko pojętego bezpieczeństwa informacyjnego, w tym np. fenomenu cyberwojny (Piasecka, 2011; Liedel, 2011; Liedel, Piasecka, 2011; Liedel, Piasecka, Aleksandrowicz, red., 2014). Warto również wspomnieć o publikacjach Krzysztofa Lidermana (2009, 2012) oraz Ernesta Lichockiego (2008, 2011). Pierwszy z nich przygotował interesujące opracowania dotyczące bezpieczeństwa informacyjnego, drugi natomiast specjalizuje się od lat w tematyce cyberterroryzmu.

Wśród literatury anglojęzycznej za najbardziej wartościowe należy uznać m.in. publikacje: Ronalda Deiberta, Rafała Rohozinskiego, Martina C. Libickiego, Patricka Hessa, Jamesa A. Lewisa, Jeffreya Carra, Johna V. Blane'a, Thomasa Rida, Richarda A. Clarke'a oraz Roberta K. Knake'a. Ron Deibert oraz Rafał Rohozinski od lat są czołowymi kanadyjskimi badaczami zajmującymi się szeroko pojętym bezpieczeństwem teleinformatycznym. Nie tylko sami są autorami wielu publikacji na ten temat, ale także prowadzone przez nich zespoły i ośrodki badawcze wsławiły się przełomowymi odkryciami w tej dziedzinie (np. chińskiej siatki szpiegowskiej *Gh0stNet*) (Deibert, 2013; Deibert, Rohozinski, 2009, 2010). Nie mniejszym uznaniem cieszy się Martin C. Libicki z RAND Corporation, który opublikował wiele opracowań dotyczących m.in. zjawiska cyberwojny czy bezpieczeństwa informacyjnego (Libicki, 2007, 2013; Dziwisz, 2013). Za bardzo

przydatne należy uznać również raporty przygotowywane przez Jamesa A. Lewisa oraz Jeffreya Carra, będących jednymi z najczęściej cytowanych amerykańskich specjalistów zajmujących się analizą incydentów komputerowych (Lewis, 2002, 2006, 2010, 2012; Carr, Rios, Plansky i in., 2009). Patrick Hess (2001) i John V. Blane (2001) zasłynęli z kolei dwoma stosunkowo dawno już opublikowanymi, lecz nadal aktualnymi opracowaniami dotyczącymi cyberterroryzmu. Nie można także pominąć Thomasa Rida (2012: 5—32; 2013), który w ostatnich latach stał się jednym z najgłośniejszych krytyków terminu *cyberwojny*. Należy ponadto wspomnieć o budzącej kontrowersje, choć zarazem bardzo przydatnej publikacji byłego doradcy prezydentów Billa Clintona i George'a W. Busha — Richarda A. Clarke'a (Clarke, Knake, 2010). Jeśli chodzi natomiast o autorów frankofońskich, to można wymienić przede wszystkim Jeana Guisnela (1997b), Limore Yagil (2002) oraz Alessandro Buffaliniego (2012).

W monografii szeroko wykorzystano opracowania opublikowane w czołowych polskich i międzynarodowych czasopismach naukowych zajmujących się m.in. bezpieczeństwem, prawem, informatyką oraz stosunkami międzynarodowymi. Wśród rodzimych periodyków, które okazały się przydatne, należy wymienić m.in.: „Stosunki Międzynarodowe — International Relations", „Bezpieczeństwo Narodowe", „Przegląd Zachodni", „Przegląd Strategiczny" czy „Sprawy Międzynarodowe". Jeśli chodzi zaś o zagraniczne, nie można pominąć takich pozycji, jak: „International Security", „Journal of Strategic Studies", „Journal of Strategic Security", „Berkeley Journal of International Law", „The Journal of International Policy Solutions", „Journal of Systemics, Cybernetics and Informatics", „International Journal of Technoethics" czy „Journal of Computers".

Praca została ponadto oparta na licznych dokumentach źródłowych, statystykach, raportach, strategiach oraz opracowaniach wydanych przez organizacje międzynarodowe (w tym Organizację Narodów Zjednoczonych, Międzynarodowy Związek Telekomunikacyjny, Sojusz Północnoatlantycki, Unię Europejską, Radę Europy czy Unię Afrykańską), instytucje i organy poszczególnych państw (koncepcje polityki zagranicznej, strategie wojskowe, strategie cyberbezpieczeństwa), ośrodki badawcze z całego świata (np. RAND Corporation, Center for a New American Century, Belfer Center for Science and International Affairs, Center for Strategic and International Studies, Chatham House, Citizen Lab), a także czołowe korporacje szeroko pojętego sektora IT (McAfee, Microsoft, Symantec, Kaspersky Lab). W pracy szeroko czerpano także, co naturalne, z danych i materiałów zamieszczanych w Internecie, przede wszystkim na portalach specjalistycznych, zajmujących się bezpieczeństwem teleinformatycznym (np. „Wired", Niebezpiecznik.pl, ZDNet). W uzasadnionych wypadkach korzystano również z witryn najważniejszych na świecie ośrodków medialnych, takich jak BBC, „The Guardian", „The New York Times" czy „The Washington Post".

Kończąc, chciałbym serdecznie podziękować wszystkim osobom, dzięki którym przygotowanie tej monografii było możliwe: przede wszystkim mojemu wieloletniemu opiekunowi naukowemu, profesorowi Mieczysławowi Stolarczykowi, kierownikowi Zakładu Stosunków Międzynarodowych w Instytucie Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego. Jego celne uwagi i wskazówki stanowiły ogromną pomoc na każdym etapie prac nad tą książką. Chciałbym również podziękować recenzentowi wydawniczemu publikacji, profesorowi Michałowi Chorośnickiemu, kierownikowi Katedry Teorii i Strategii Stosunków Międzynarodowych w Instytucie Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego. Jego cenne sugestie pozwoliły znacząco podnieść poziom merytoryczny prezentowanej monografii. Za pomoc dziękuję także Andrzejowi Kędzierskiemu, kierownikowi Sekcji Informatycznej Sądu Rejonowego w Będzinie, który zgodził się pełnić rolę konsultanta technicznego, dzięki czemu udało się wyeliminować szereg błędów i nieścisłości z pierwotnej wersji tej rozprawy. Wyrazy wdzięczności kieruję także w stronę International Council for Canadian Studies, dzięki któremu w 2011 roku byłem w stanie zrealizować grant naukowy poświęcony cyberbezpieczeństwu Kanady. Zdobyte podczas pobytu w Toronto doświadczenia okazały się bardzo przydatne w badaniach nad rywalizacją i współpracą państw w cyberprzestrzeni. Serdecznie dziękuję również władzom Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego oraz Wydziału Nauk Społecznych Uniwersytetu Śląskiego za wyasygnowanie środków, dzięki którym publikacja ta mogła ukazać się w druku.

Indeks osobowy

Abelson Philip H. 43, 429
Achenbach Joel 69, 429
Adamowski Janusz 429, 431, 436, 446, 448
Adams James 8, 430
Adamski Andrzej 29, 30, 33, 37, 39, 56
Agarwal Ashok 429, 438
Ahuja Abha 89, 461
Akayev Askar 228, 429
Akera Atsushi 429, 436
Alberts David S. 30, 33, 52, 62, 112, 429, 431, 432, 435, 438, 443, 445—449
Albright David 261, 453
Aleksandrowicz Tomasz R. 21, 103, 166, 429—430, 442, 445—448
Alexander Keith B. 165, 327, 430
Alkassar Ammar 430, 450
Alperovitch Dmitri 320, 321, 453,
Anderson Robert H. 47, 58, 60, 69, 438
Anderson Ross J. 132, 150, 151, 439, 453
Andes Scott 59, 435
Anokhin Mikhail A. 16, 430
Arbatow Aleksiej 187
Arcari Maurizio 430, 432
Armstrong Charles K. 277, 430
Arquilla John 94, 167, 171, 180, 430
Asghari Hadi 414, 450
Ashmore William C. 202, 234, 235, 430
Ashton Catherine 81, 388, 389, 453, 454, 464
Aspray William 429, 436
Atkinson Robert D. 58, 454
Auvinen Ari-Matti 454
Avgerou Chrisanthi 431, 432
Avila Alfonso 415, 430

Balcerowicz Bolesław 15, 16, 137, 169, 177, 178, 430, 434, 437, 438, 440, 442, 448
Baldwin David A. 15, 430
Balmond Louis 430, 432
Bania Radosław 80, 103, 174, 252, 261, 262, 430, 445
Baocun Wang 309, 430
Baram Gil 255, 430
Barańska Bogumiła 61, 430
Barcz Jan 430, 436, 444
Barletta William A. 198, 430, 450
Barton Christ 150, 151, 453
Bateson Gregory 75
Bauer Johannes M. 414, 449, 450
Bautzmann Alexis 133, 165, 431
Bédar Saïda 111, 431
Bell Daniel 26, 431
Bencsáth Boldizsar 264—266, 431, 454
Bendiek Annegret 112, 133, 379, 454
Bentley Alan 256
Berkowitz Bruce 98, 101, 165, 431
Berleur Jacques 431, 432
Berman Czesława 27

Bidgoli Hossein 130, 459
Bieleń Stanisław 185, 186, 431
Bieńczyk-Missala Agnieszka 15, 440
Bierzanek Remigiusz 117, 119, 135, 154, 177, 200, 340, 410, 415, 431
Bikson Tora K. 47, 58, 60, 69, 438
Billo Charles G. 114, 133, 174, 281, 284, 431, 454
Bimber Bruce 7, 431
Blane John V. 21, 22, 133, 171, 431, 437
Bobrow Davis B. 15, 70, 431, 437, 439, 442, 444
Bogdański Andrzej 112, 431
Bohlen Celestine 211, 451
Boland Julie 402, 454
Bolter David J. 43, 431
Borger Julian 106, 167, 451
Borghello Cristian 108, 459
Boulding Kenneth E. 26, 431
Bógdał-Brzezińska Agnieszka 16, 21, 36, 61, 62, 67, 78, 83, 101, 124, 126, 143, 145, 157, 160, 190, 379, 410, 431
Böhme Rainer 150, 151, 453
Brannan Paul 261, 453
Brągoszewski Paweł 108, 451
Brennan John W. 159, 160, 454
Brodeur Jean-Paul 435, 441
Bronk Christopher 171, 328, 431
Bryc Agnieszka 185, 211, 432
Bryła Jolanta 13, 432, 443
Brzeziński Zbigniew 42, 432
Bufalini Alessandro 133, 165, 432
Bugubajew Kubungazy 229, 231
Bullen Elizabeth 43, 439
Bult Jeroen 184
Bumblauskas Afredas 203, 434
Bumiller Elisabeth 160, 307, 451
Burgess Ronald L. 253, 454
Burnham David 43, 432
Buttyán Levente 264—266, 431
Byres Eric P. 259, 454

Camiña Steven 76, 443
Caplan Nathalie 273, 432
Carr Jeffrey 21, 22, 34, 106, 133, 167, 171, 223, 234, 236, 262, 283, 311, 313, 324, 432, 454
Cartwright James E. 122, 314, 454
Castells Manuel 34, 40, 45, 47, 48, 58—60, 64, 432
Castro Daniel 59, 67, 455
Cerf Vinton G. 37, 39, 40, 441
Chamberlain Nigel 375, 432
Chang Welton 67, 114, 133, 174, 281, 283, 431, 442, 454
Chang-Il Ohn 276, 432
Chanlett-Avery Emma 277, 278, 432, 455
Chen Xinxiang 307, 432
Chenok Daniel 304, 464
Chien Eric 256, 257, 263, 458
Choi Rodney 155, 156, 463
Chou Shihchieh 67, 442
Choucri Nazli 76, 443
Christakis Dimitri A. 49, 432
Clark David D. 39, 40, 403, 441, 448
Clarke Richard A. 21, 22, 73, 77, 94, 105, 107, 133, 165, 167, 175, 179, 200, 217, 248, 282—285, 308, 310, 326, 344, 432
Clarke Zuley 104, 139, 432
Clawson James 104, 139, 432
Clayton Richard 150, 151, 453
Clemente Dave 261, 432
Coeira Enrico 59, 432
Cohen Gili 147, 451
Cohen-Almagor Raphael 32—34, 41, 42, 45, 46, 48, 432
Colarik Andrew 175, 432
Coleman Kevin 99, 108, 283, 455
Collins Kathleen 229, 432
Comer Douglas E. 33, 39, 41, 52, 56, 86, 87, 88, 432
Conley Heather A. 185, 188, 435, 455
Conway Maura 144
Copeland Tomas E. 431, 432, 434, 436, 438, 444, 446
Cordell Maria 104, 139, 432, 455
Cordesman Anthony H. 8, 98, 167, 241, 244, 326, 432, 455
Cordesman Justin G. 8, 98, 167, 326, 432, 455
Cornish Paul 174, 261, 432, 455
Coroalles Anthony M. 111, 448
Creedon Madelyn R. 112, 433
Crootof Rebecca 112, 273, 437

Cutts Andrew 117, 433
Czachór Zbigniew 13, 443
Czaputowicz Jacek 15, 16, 433
Czebotar Łukasz 307, 433
Czermiński Alfred 117, 135, 433
Cziomer Erhard 13—15, 97, 433
Czornik Katarzyna 238, 240, 242, 299, 433
Czosseck Christian 108, 433, 435—437, 441, 442, 444, 447, 449, 450

Dacier Marc 449
Dahrendorf Ralf 26
Dajani Muna 239, 456
Dalton Melissa G. 252, 460
Dasgupta Dipankar 123, 132, 466
David Michela 188, 455
Davis Joshua 191, 198, 451
Dawidziuk Patryk 66, 433
de Haas Marcel 400, 433
Deibert Ronald J. 21, 34, 67, 71, 163, 314, 315, 344, 433, 457
Delpech Thérèse 111, 433
Delvy Pierre 76
Denning Dorothy E. 144, 156, 160, 206, 433, 457
Deutsch Karl 177
Devost Matthew G. 8, 223, 434, 454
Dietz J. Eric 442
Diffie Whitfield 403, 449
Dobroczyński Michał 13, 434
Dobrosielski Marian 14
Doktorowicz Krystyna 67, 434
Dolven Ben 301, 457
Dornheim Michael A. 246
Dowty Alan 238, 434
Drake William 59, 434
Drucker Peter F. 451
Drzyzga Piotr 434, 445
Dunn-Cavelty (Dunn) Myriam A. 10, 26, 44, 65, 73, 93, 101, 104, 106, 111, 139, 165, 167, 434
Durkalec Jacek 434
Dutta Soumitra 238, 457
Dyduch Joanna 242, 434
Dzisiów-Szuszczykiewicz Aleksandra 240, 434
Dziwisz Dominika 21, 304, 307, 434

Eagle Chris 312, 437
Eidintas Alfonsas 203, 434
Eisenstadt Michael 254, 457
Ellis Bryan W. 95, 368, 458
Ellis Charles 123, 132, 466
Emm David 258
Eom Gu-Ho 212, 439
Eriksson Johan 8, 64, 434
Esquibel Elijah J. 126, 153, 458
Evans Karen S. 304, 464
Even Shmuel 161, 261, 435
Ezell Stephen 59, 435

Fahey Jonathan 43, 439
Faissol Daniel 118, 124, 125, 130—132, 462
Fajgielski Paweł 67, 435
Falkowski Maciej 212, 458
Falliere Nicolas 256, 257, 263, 458
Farivar Cyrus 195, 435
Feakin Tobias 284, 294, 297, 327, 435, 458
Fei Li 309, 430
Félegyházi Márk 264—266, 431, 454
Ficoń Krzysztof 117, 135, 433
Filip Andrzej 88
Fink Charles A. 75
Finklea Kristin M. 77, 95, 151, 458
Fiore Quentin 26, 443
Fisher Richard 327, 458
Fitchett Joseph 120, 452
Fitri Nofia 144, 435
Fogelman Martin 67, 435
Foltz Andrew C. 262, 435
Foster-Carter Aidan 277, 435
Fötinger Christian S. 120, 458
Friedberg Aaron 303
Fronczek Mariusz 62, 449
Fulgham David A. 245, 246
Fulmański Piotr 29, 38, 43, 85, 435

Gacek Łukasz 303, 435
Gagnon Benoît 140, 435
Gagnon Greg 156, 463
Gallis Paul 213, 458
Gała Katarzyna 15, 435
Gao Jiaqing 307, 432

Garstka John J. 112, 429
Gartzke Erik 8, 273, 435
Gasparini-Alves Péricles 347, 435
Gasperre Richard B. 246, 247
Gawrycki Marcin Florian 16, 62, 83, 101, 126, 190, 379, 410
Gawrysiak Piotr 30, 51, 55, 435
Geers Kenneth 29, 9, 94, 113, 147, 171, 193, 275, 325, 425, 433, 435, 437, 441, 444, 447, 449, 458
Gellman Barton 68, 325, 452
Gerber Theodore P. 185, 188, 435, 455
German Tracey C. 211, 213—214, 435, 436
Gertler Jeremiah 254, 469
Giacomello Gianpiero 8, 64, 434
Gibson William 72, 139, 436
Giddens Anthony 26, 436
Giles Keir 102, 165, 342, 436,
Ginter Andrew 259, 454
Givner-Forbes Rebecca 223, 454
Gjelten Tom 328, 362
Glabus Edmund M. 436
Goban-Klas Tomasz 21, 29, 31, 40, 52, 54—55, 59—61, 63, 68, 69, 86, 436
Gogolashvili Kakha 436, 447
Gogołek Włodzimierz 58, 436
Golding Peter 30
Goodman Seymour 408, 445
Gostiew Aleksander 128, 452
Gottlieb Benjamin 141, 452
Graham Bradley 163, 452
Grącik Małgorzata 433, 451
Green James L. 36, 436
Griffin Em 436
Grishin Oleg 16, 430
Grochmalski Piotr 211, 436
Gross Michael J. 273, 452
Grosse Tomasz G. 300, 436
Grönlund Åke 62, 438
Grzebyk Patrycja 15, 440
Grzelak Agnieszka 379, 436
Grzelak Michał 325, 329, 436
Grzybowski Marek 117, 135, 433
Gu Qijin 459
Guisnel Jean 8, 22, 40, 111, 138, 140, 166, 170, 436
Gulbas Karol 436
Gupta Keshav Dev 245, 436
Haber Lesław H. 430, 434, 436—438, 441, 444—447, 449, 450
Haigh Thomas 31, 436
Hair Dwight 36, 447
Halfond William G.J. 131, 132
Haliżak Edward 13, 15, 16, 278, 303, 430, 431, 434, 437—440, 442, 444, 448
Haltmaier Jane 299, 437
Hammond Allen L. 43, 429
Hampson Noah C.N. 120, 437
Hansman Simon 123, 437
Hare Forrest 78, 368, 437
Harley David 108, 126, 158, 459, 462
Harmon Glynn 27
Harper Allen 141, 437
Harris Shon 141, 437
Hassan Jawad 194, 197, 466
Hathaway Oona A. 122, 273, 437
Hauben Michael 139, 452
Haynes Colin 124, 443
Healey Jason 118, 181, 371, 376, 459, 464
Heinl Caitriona H. 8, 437
Heintschel von Heinegg Wolff 272, 368, 437
Herz John H. 15, 437
Herzog Stephen 199, 202, 437
Hess Patrick 21, 22, 133, 437
Hetmański Marek 59, 437
Hildreth Steven A. 76, 106, 254, 309, 437, 469
Hinnebusch Raymond 239, 240
Hirschauge Orr 147, 451
Hjortdal Magnus 327, 437
Hoffmann Romuald 74, 165, 445
Hollis David 168, 215, 217, 220, 224, 438
Holsti Kalevi Jaakko 13, 438
Holt Thomas J. 433, 438
Hong Zao 299, 459
Hoon Lee Dong 283
Horan Thomas A. 62, 438
Houghton Brian K. 8, 434
Huasheng Zao 299, 459
Huber Peter 112, 438
Hui Sylvia 302, 459

Hundley Richard O. 47, 58, 60, 69, 438
Hunt Ray 123, 437

Iacobucci Michael 156, 463
Irvine Matthew 252, 460
Isenberg David 98, 438

Jackson Don 234, 235
Jahanian Farnam 89, 461
Jain Palvia Shailendra C. 62, 438
Jakubski Krzysztof J. 151
Janczak Józef 16, 438
Janczewski Lech 175, 432
Jarczewska Aleksandra 300, 438
Jas Marta 429, 431, 436, 446, 448
Jawasreh Median 239, 438
Jen WenYuan 67, 442
Jeran Agnieszka 27, 438
Jincheng Wei 308
Johansson Karsten 125
Jordan Tim 123, 138, 139, 144, 438
Joshi Jitendra 245, 436
Joubert Vincent 147, 189, 196, 438, 460

Kaczmarski Marcin 298—300, 438
Kahl Collin H. 252, 460
Kahn Robert E. 39, 40, 441
Kallberg Jan 112, 169, 438
Kambil Ajit 34, 438
Kan Shirley A. 298, 460
Kanuck Sean 95, 402, 438
Kanwal Gurmeet 309, 438
Kapuśniak Tomasz 435, 438, 444, 449
Karabeshkin Leonid A. 204, 460
Kasekamp Andreas 439, 442
Kaska Kadri 216—219, 224—226, 468
Kastenberg Joshua E. 225, 439
Katz Irvin R. 75, 439
Katzman Kenneth 254, 469
Kaye Dalia Dassa 251, 254, 460
Kearns Ian 206, 466
Kemp III W. Thomas 52, 429
Kenway Jane 43, 439
Kerr Paul K. 251, 253, 460
Kert Mari 216—219, 224—226, 468
Kępa Leszek 131, 247, 439
Khan Robert 34
Kim Duyeon 287, 460
Kim Samuel S. 276—279, 461
Kim Younkyoo 212, 439
Kirch Aksel 186, 461
Kirk Don 279 452
Kitler Waldemar 15, 439
Kiwerska Jadwiga 300, 439
Kjaerland Maria 124, 439
Klein Gabriel 108, 433
Kleinrock Leonard 32, 33, 39—40, 441
Knake Robert K. 21, 22, 77, 94, 104, 165, 175, 179, 200, 217, 248, 283—285, 308, 310, 326, 432
Knights Michael 254, 457
Koehan Robert 15
Kołodziej Edward A. 15, 439
Kondrakiewicz Dariusz 13, 439
Korns Stephen W. 225, 439
Kosmynka Stanisław 159, 439
Kostecki Wojciech 13, 439
Kotowicz Krzysztof 131
Kowalkowski Stanisław 15, 439
Koyama Kenichu 43
Kozłowski Andrzej 21, 449
Kramer Franklin D. 439
Krekel Bryan 311, 312, 328, 461
Krepinevich Andrew W. 8, 199, 201, 461
Kronenfeld Sami 466
Kshetri Nir 401, 439
Kuchins Andrew C. 299, 459
Kuehl Daniel T. 8, 9, 77, 112, 439, 444
Kuhn Marcus G. 132, 439
Kukułka Józef 13, 15—16, 440, 445
Kulakauskas Antanas 203, 434
Kulesa Łukasz 274, 440
Kuprejew Oleg 255, 256
Kurowski Wojciech 118, 119, 440
Kuźniar Roman 15, 430, 434, 437, 438, 440, 442, 448

Laasme Häly 367, 440
Labovitz Craig 89, 461
Lafargue François 299, 440
Lai Robert 308, 328, 331, 440
Lakomy Miron 95, 102, 106, 107, 116, 135, 137, 140, 141, 150, 153, 157, 160, 162—164, 166, 168, 170, 175, 196, 213,

214, 215, 227, 251, 253, 304, 305, 440, 441
Lakomy Mirosław 33, 36, 41, 47, 48, 62, 63, 440, 441
Lamberton Donald M. 43, 441
Langill Joel 259, 454
Langner Ralph 258—260, 262, 461
Larson Dean 166, 442
Latoszek Ewa 379, 441
Laurenzano Michael A. 126, 153, 458
Laurinavičius Česlovas 203, 461
Leder Felix 108, 433, 441
Lee Andrew 108, 126, 459
Leiner Barry M. 39, 40, 441
Lekowski Maciej 167, 441
Leman-Langlois Stéphane 435, 441
Lesk Michael 191, 461
Leszczyńska Małgorzata 57, 441
Leszczyński Marek 16, 441
Levi Michael 150, 151, 453
Levitz Philip 122, 273, 437
Levy Steven 138, 139, 441
Lewis James A. 8, 21, 22, 103, 156, 160, 172, 173, 228, 271, 304, 308, 326, 347, 461, 464
Liang Qiao 309, 441
Liba Itai 291, 466
Libicki Martin C. 21, 82, 83, 97, 156, 368, 434, 441
Lichocki Ernest 21, 78, 157, 441, 461
Liderman Krzysztof 17, 21, 65, 73, 74, 87, 130, 133, 155, 441
Liedel Krzysztof 16, 17, 21, 27, 55, 63, 70, 100, 103, 117, 127, 133, 148, 161, 163, 166, 171, 173, 180, 429, 430, 441, 442, 445—448
Liles Samuel 166, 442
Lipson Howard F. 95, 461
Liu Peng 130, 459
Livingstone David 261, 432
Lizak Wiesław 16, 240, 243, 435, 442, 444
Long Austin 238, 446
Lopez-Claros Augusto 238, 457
Lord Kristin M. 464
Lu Chichao 67, 442
Lucky Robert W. 8, 452
Lulu Chang 302, 451
Lunn Simon 206, 466
Lynch Daniel 39, 40, 441

Łapiński Aleksander 128, 452
Łącki Borys 66, 108, 433
Łebkowska Joanna 15, 442
Łopińska Aleksandra 302, 442
Łoś-Nowak Teresa 13, 14, 16, 279, 434, 442, 443, 451

Made Vahur 187, 188, 442
Madej Marek 15—17, 21, 27, 54, 57, 64, 65, 69, 70, 78, 89, 90, 116, 133, 134, 431, 433, 440, 442, 443, 447, 449
Madnick Stuart 76, 443
Mahoney Michael S. 54, 443
Malcho Juraj 158, 462
Malendowski Włodzimierz 13, 14, 432, 436, 438, 443, 444
Mambetalieva Tattu 233
Mansourov Alexandre 284
Manyin Mark E. 301, 457
Marbach William D. 139, 452
Marke John 246
Marszałek-Kawa Joanna 301, 443
Martin James 42, 443
Martini Peter 108, 441
Marx Leo 431, 447
Matera Paulina 300, 302, 443
Matray Jamers I. 277, 443
Matrosov Aleksandr 158, 462
Mattioli Andrea 66, 450
Matyska Piotr 221, 222
Mauchly John W. 29, 85
Maurer Tim 67, 135, 154, 336, 337, 344, 346, 361, 462
Mazarr Michael J. 111, 443
Mazur Marian 75, 443
McAfee John 124, 443
McDonald Geof 318, 463
McFadden Robert D. 298, 452
McGrady Ryan 130, 144, 469
McKay Andrew S. 58, 454
McLuhan Marshall 26, 60, 443
Mees Wim 108, 449
Mehan Julie E. 64, 108, 156, 174, 443
Mehlinger Howard D. 59, 443

Meikle Graham 144
Mele Stefano 127, 462
Melnitzky Alexander 82, 112, 164, 443
Melzer Nils 77, 112, 175, 340, 462
Meridian Dyn 98, 438
Messner Zbigniew 27, 443
Metz Steven 70, 112, 444
Meyers Carol 118, 124, 125, 130, 131, 132, 462
Mia Irene 238, 457
Michałowska Grażyna 16, 444
Migdalovitz Carol 243, 462
Miller Charlie 66, 462
Miller Robert A. 9, 444
Milone Mark G. 144, 444
Miłostan Maciej 105
Miniotaitė Gražina 204, 462
Miszczak Krzysztof 379, 444
Mitchell Mark 155, 156, 463
Moćkun Sławomir 106, 133, 198, 462
Mojsiewicz Czesław 13, 15, 432, 443, 444
Molander Roger C. 76, 96, 97, 112, 164, 170, 444
Moore Lucy 185, 188, 435
Moore Tyler 150, 151, 453
Moran Ned 223, 454
Morrison Wayne M. 298, 460
Mulliner Colin 66, 462
Mulvenon James C. 313, 314, 327, 331, 462
Murdock Graham 30
Murray Williamson 111, 444
Myrli Sverre 167, 181, 197, 366, 369, 374, 463
Myszczyn Janusz 27, 444
Myszczyn Wioletta 27, 444

Nachev Atanas 444
Nader Alireza 251, 254, 460
Nakashima Ellen 159, 452
Nakhleh Hany T. 243, 463
Nazario Jose 192, 217, 220, 234, 236, 285, 286, 424, 444
Neilson Reid E. 434, 444
Nekrašas Evald 203, 444
Nelson Bill 155, 156, 463
Nerguizian Aram 241, 244, 455
Ness Jonathan 141, 437
Neu C. Richard 47, 58, 60, 69, 438
Nichol Jim 215, 227, 230, 232, 463
Niezgoda Marian 61, 444
Nikitin Mary Beth 277, 278, 463
Nikolov Eugene 124, 444
Nix Haley 122, 273, 437
Noor Elina 155, 444
Norman Adrian R.D. 42, 443
Nowak Andrzej 16, 438
Nowak Eugeniusz 16, 115, 444
Nowak Maciej 16, 115, 444
Nowiak Joanna 13, 444
Nowlan Aileen 122, 437

O Murchu Liam 256, 458
O'Connell Mary Ellen 101, 444
O'Gorman Gavin 318, 463
Ociepka Beata 13, 444
Olszewski Paweł 435, 444
Orso Alessandro 131, 132
Ostaszewski Marek 62, 449
Ottis Rain 433, 436, 437, 442, 449, 450

Pacek Bogusław 165, 445
Paget François 121, 146, 149, 445, 463
Palfrey John 130, 469
Paller Alan 304, 313, 464
Pandey Sheo N. 311, 463
Papp Daniel S. 30, 33, 62, 429, 431, 432, 435, 438, 443, 445, 446, 447—449
Park Jae-Kyung 301—303, 463
Pawlak Marcin 257
Pawlikowska Iwona 16, 445
Pék Gabor 264—266, 431, 454
Perdue William 122, 437
Petkova Gergana 147, 460
Piasecka Paulina 21, 117, 127, 133, 148, 163, 171, 173, 180, 181, 429—430, 442, 445—448
Piech Krzysztof 444, 445
Pietraś Marek 15, 16, 437, 439, 444, 445
Piotrowski Marcin Andrzej 237, 242, 250, 445
Pkhaladze Tengiza 447
Plansky Derek 22, 223, 454
Pocius Edvardas 208
Podraza Andrzej 133, 433

Pogońska-Pol Magdalena 239, 445
Poitras Laura 68, 452
Pollard Neal A. 8, 434
Popescu Adam 364
Popescu Ionut C. 241, 244, 455
Popiuk-Rysińska Irena 13, 445
Popławski Dariusz 430, 434, 437, 438, 442, 448
Porębski Leszek 62, 445
Portnoy Michael 408, 445
Postel Jon 39, 40, 441
Potakowski Paweł 433—435, 439, 441, 445, 447, 448, 450
Poulsen Kevin 195
Powers Sarah 118, 124, 130, 131, 132, 462
Presper Eckert John 29, 85
Pronińska Kamila 15, 440
Przybycień Krzysztof K. 59, 445
Przybylska-Maszner Beata 440, 446
Psaki Jen 350, 464
Pudełko Marek 31—33, 35, 39—42, 46, 48, 58, 69, 446
Pufeng Wang 308, 446

Raas Withney 238, 446
Rabinovich Itamar 242, 243, 464
Rahman Syed 308, 328, 331, 440
Ramana V. Venkata 429, 438
Rattray Greg J. 118, 464
Record Jeffrey 165, 446
Reeder Franklin S. 304, 464
Regina-Zacharski Jacek 177, 446
Reid Donald N. 313, 464
Repko Elliot M. 240, 446
Rękawek Kacper 21, 449
Richards Jason 191, 192, 446
Rid Thomas 21, 22, 77, 133, 168, 171, 172, 249, 446
Riddile Andrew S. 76, 96, 97, 112, 164, 170, 444
Rinehart Ian E. 277, 278, 432, 455
Rios Billy 22, 223, 454
Rischard Jean-François 44, 446
Robb Simon 43, 439
Roberts Hal 130, 144, 469
Roberts Lawrence G. 39, 40, 441
Robinson A. 155, 465
Robinson James 44, 446
Rodionov Eugene 158, 462
Rogers Marcus 166, 442
Rohozinski Rafał 21, 163, 236, 315, 457
Rona Thomas 171
Ronfeldt David 94, 167, 171, 180, 430
Rorive Isabelle 397, 446
Roscini Marco 95, 446
Rosen Christine 64
Rosenau James N. 54, 446
Rosenfield Daniel K. 199, 446
Roshan Parisa 251, 254, 460
Roszczynialski Włodzimierz 59, 446
Rothert Agnieszka 31, 34, 77, 79, 446
Rutkowski Piotr 392, 446
Ruus Kertu 149, 184, 367, 446
Rünnimeri Kristel 216, 217—219, 224—226, 468
Ryan Marie Laure 76

Saalbach Klaus-Peter 97, 111, 121, 175, 446
Saco Diane 446
Saleem Muhammad 131, 194, 197, 466
Salem Paul 239, 240, 466
Sampson R. Neil 36, 447
Sandvik Kristin Bergtora 95, 447
Sapetkaitė Vaiva 207
Saramak Bartosz 95, 447
Savage Stefan 150, 151, 453
Schackelford Scott J. 195, 198, 447
Schell Bernadette H. 433, 438
Schmitt Michael N. 81, 121, 122, 373, 447
Schreier Fred 77, 78, 93, 96, 100, 118, 166, 167, 172, 175, 225, 248, 261, 466
Schweitzer Yoram 133, 447
Scott William B. 246
Segal Robert L. 58, 447
Senghaas Dieter 177
Seongho Sheen 278, 466
Shafie Shamsul Jafni 407, 409, 466
Sharikov Pasha 341, 343, 466
Sharma Amit 62, 111, 447
Sharma Sushil S. 62, 438
Sharp Travis 464
Sherstobitoff Ryan 291, 466
Shetty Shatabhisha 127, 206, 406
Shimeall Timothy 101, 133, 171, 447

Shiva Sajjan 123, 132, 466
Shramko Zlata 233
Siboni Gabi 133, 272, 447, 466
Sienkiewicz Piotr 21, 27, 29, 31, 40, 52, 54, 59, 61, 63, 68, 69, 86, 106, 113, 118, 119, 121, 133, 136, 153, 164, 166, 171, 436, 447
Silaev Nikolai 212, 447
Silicki Krzysztof 134, 447
Silverstein Shannon 223, 454
Siman-Tov David 161, 261, 435
Simmons Chris 123, 132, 466
Simon Steven 242, 466
Siwicki Marek 99, 151, 336, 379, 410, 447
Skrzypczak Jędrzej 99, 447
Skwarzyński Michał 67, 447
Smith David J. 226, 466
Smith Merritt Rose 431, 447
Smith-Bers Joanna 58, 77, 448
Smith-Macklin Alexius 75, 439
Sobieski Ścibór 29, 38, 43, 85, 435
Sofaer Abraham D. 403, 448
Sokała Witold 101, 448
Sokolski Henry D. 95, 448
Soltanifar Mohammad 212, 448
Sorel Georges 177,
Spafford Eugene 171, 172
Spiegel Julia 122, 437
Squassoni Sharon 250, 466
Stachura Jadwiga 252, 299, 448
Stanley Nigel 190, 466
Starr Stuart H. 439
Stefanowicz Bogdan 27, 448
Stefanowicz Janusz 13, 434
Stein Frederick P. 112, 429
Sterner Eric 144, 448
Stępień Tomasz 56, 448
Stolarski Marek Piotr 66, 433
Storch Tyson 131, 466
Suchorzewska Aleksandra 64, 448
Sullivan Gordon R. 111, 448
Sułek Mirosław 15, 440, 448
Swanson Lesley 227
Symonides Janusz 117, 119, 135, 154, 177, 200, 302, 303, 340, 410, 415, 431, 448
Szarfenberg Ryszard 59, 448
Szczodrowski Grzegorz 444, 445
Szeptyński Piotr 56, 448
Szlajfer Henryk 430, 434, 437, 438, 442, 448
Szpunar Magdalena 26, 64, 69, 448
Szubrycht Tomasz 92, 112, 156, 448
Szymański Tomasz 92, 448
Szymczyk Katarzyna 250, 251, 253, 449
Szyszłak Tomasz 187, 449

Świeboda Halina 21, 113, 118, 119, 121, 133, 153, 164, 166, 171, 447
Šmihula Daniel 53, 58, 447

Tabansky Lior 127, 449
Tabatabaie Shirin 414, 450
Tabor Marek 440
Taddeo Mariarosario 57, 449
Tafoya William L. 156, 467
Tailhärm Anna-Maria 216—219, 224—226, 468
Tamošaitis Mindaugas 203, 434
Tan Wenda 307, 432
Tarakanov Dmitry 293
Tarnogórski Rafał 394, 449
Taylor Paul 33, 144, 438
Tchórzewski Jerzy 62, 449
Telang Rahul 66, 449
Terlikowski Marcin 17, 21, 67, 116, 117, 133, 134, 139, 142, 145, 154, 156, 221, 431, 433, 442, 443, 447, 449
Theohary Catherine A. 77, 95, 151, 458
Thonnard Olivier 108, 449
Thornburgh Nathan 313, 452
Tikk Eneken 205, 206, 216—219, 224—226, 367, 449, 468
Timlin Katrina 347, 461
Toffler Alvin 26, 53, 70, 449
Topolski Ireneusz 186, 187, 203, 449
Touré Hamadoun 353, 359—362, 364, 434, 449, 450
Trejderowski Tomasz 100, 131, 140, 145, 156, 449
Treschel Alexander H. 189, 468
Troitskiy Jegwienij 229—231
Tuyahov Alissa 30, 33, 445
Tyugu Enn 433, 436

Ulasen Sergey 255
Umesamo Tedao 43
Ursuł Arkadij D. 27

Vamosi Robert 144
Van Bochoven Leendert 181, 371, 376, 459
Van der Dennen J.M.G. 177, 469
Van der Putten Frans-Paul 400, 433s
Van Eeten Michel J.G. 150, 151, 414, 449, 450, 453
Viegas Jeremy 131, 132
Vihul Liis 216—219, 224—226, 468
Villafiorita Adolfo 66, 450
Vinge Vernor 72, 450
Volkamer Melanie 430, 450
Von Bogdandy Armin 446, 450
Von Clausewitz Carl 176, 178, 450
Von Neumann John 85

Wall David S. 9, 96, 134, 156, 450
Walrond Christina 261, 453
Walter James 291, 466
Walton Greg 223, 454
Warden John A. 164, 450
Warrick Joby 159, 452
Wattal Sunil 66, 449
Watts Sean 68, 273, 450
Weathersby Kathryn 276, 450
Wegener Henning 430, 450
Weimann Gabriel 8, 450
Weldemariam Komminist 66, 450
Wentz Larry K. 439
Werner Tillman 108, 441
Westby Jody R. 357, 361, 430, 450
Wiak Krzysztof 433—435, 439, 441, 444, 445, 447, 448, 450
Wiener Norbert 27, 74, 75
Willson David L. 197, 450
Wilson Clay 130, 155, 157, 158, 469
Wilson Peter A. 76, 96, 97, 112, 164, 170, 444
Wilson Zachary 66, 469
Wingfield Thomas C. 77, 433, 436, 469
Włodowska-Bagan Agata 15, 450
Wojciechowski Sebastian 119, 450
Wojciuk Anna 15, 440
Wolfers Arnold 15, 450
Wolff Stephen S. 39, 40, 441
Wolfrum Rudiger 446, 450
Woon Wei Lee 76, 443
Wortzel Larry M. 328, 329, 331, 450, 469
Woźniak Michał G. 441, 450
Wright Quincy 177
Wu Qishi 123, 132, 466
Wu Timothy S. 368, 450
Wynn Michael 77
Wytrążek Wojciech 62, 450

Xiangsui Wang 309, 441
Xiao Jing 126, 153, 458
Xu Ting 326, 469

Yagil Limore 22, 125, 126, 129, 140, 170, 450
Yogev Einav 133, 447
York Jillian 130
Yorke Claire 261, 432

Zacher Lech W. 61, 450
Zając Justyna 14, 15, 239, 298, 432, 438, 450, 451
Zając Krzysztof 13, 62, 449
Zakrzewski Arkadiusz 129, 452
Zakrzewski Stanisław 16, 451
Zanotti Jim 242, 254, 469
Zawojski Piotr 60, 61, 451
Zdulski Krzysztof 430, 445, 449
Zhang Li 310, 451
Zhao Suisheng 302, 451
Zhimin Chen 302, 451
Ziarek Maciej 128, 273, 452
Ziegler Wolfgang 120, 458
Zięba Ryszard 13—15, 431, 437, 439, 442, 444, 445, 450, 451
Ziolkowski Katharina 425, 433, 436, 442, 449, 451
Ziomka Zbigniew 152, 469
Zuckerman Ethan 144, 469
Zuvich Ted 126, 153, 458
Zyblikiewicz Lubomir W. 433

Żukrowska Katarzyna 16, 433, 451
Żurawski vel Grajewski Przemysław 137, 177, 178, 180, 451

Miron Lakomy

Cyberspace as a new dimension of competition and cooperation between countries

Summary

The computer revolution which started in the second half of the 20th century has significantly changed the world in almost every possible aspect and dimension within only a few decades. As it was predicted by some technological determinists, the processes of computerization and IT technologies' implementation have quickly included the consecutive areas of life of individuals and their communities, starting from economy, through science and entertainment, to politics and military service. In terms of the most conspicuous features, such as the overcoming of the previous limitations in processing, sending and storing information, it has brought enormous benefits to humanity. The development of a new unique domain that the cyberspace represents, has become their symbol. Owing to its specific features, for decades it has been determining the functioning of countries and communities to an ever growing extent, permeating the state administration, critical infrastructure, business sector and, finally, armed forces. Their growing dependence on ICT, however, has simultaneously become the reason for the emergence of certain negative tendencies, the cost of which is paid around the world. The universality and global character of information and communication technologies has led to some breakthroughs in the broadly understood safety dimension. Computers and their networks, contributing to the revolution in military affairs (RMA), have at the same time become the source and the platform for the destructive phenomena which, with time, started to be perceived through the prism of a threat to the national and international security. Various individuals, starting with average amateurs, hackers, through hacktivists, cyber-terrorists, and ending with criminal organizations, have gained a prospective possibility to reach even the most vital spheres of the particular countries' security systems owing to cyberspace. In other words, cyberspace has paradoxically become another safety dimension, the role of which has been increasing in proportion to the advances in the processes of computerization and IT technologies' implementation. Still in the 90s of the 20th century, even the most serious computer attacks were usually regarded as, at most, certain nuisance for the central administration, whereas already two decades later, their range has

become large enough to be seen as one of the most serious challenges to the stability of the whole international system.

In this new environment which cyberspace constitutes, these countries which until recently have not evinced any broader interest in the development of skills allowing them to become active in that field, remain the most unique subjects. It started to change at the turn of the 20th and 21st century, when the potential benefits that may be brought by cyberspace became recognized by the political elites of several countries, such as the United States, Russia, China or Israel. On the one hand, the works on the development of the professional and technological potential have been initiated, which allowed for the creating of a more effective security system against computer web breakings. On the other hand, it has been acknowledged that the offensive activeness in teleinformatic sphere may become a convenient weapon in the competition and confrontation with other subjects within the international environment. The objective characteristics of this domain, such as: easily accessed anonymity, "a-geographicity" and "a-territoriality" or low costs of "entry," favoured it. Moreover, the ambiguities connected with interpretation of the binding regulations of international law and mechanisms of political and military cooperation confirmed usefulness of these tools. In only a few years the forerunners have developed very advanced skills in that field, which, in theory, could serve the realization of particular aims in selected specializations.

In this context, the presented study is an attempt to discuss the efficiency of teleinformatic means as the instruments of foreign policy of countries during the post-Cold War period. Taking into account aspects of both competition and cooperation of governments in cyberspace, in the conducted analysis the elements of the theory of foreign policy have been used. The dissertation contains primarily a discussion on the essence and the particular stages of digital revolution which has led to the development of teleinformatic space. Then, its most important features have been characterized from both technical and politological perspectives. On this basis, an attempt to create a simplified typology of teleinformatic dangers to the countries' security has been undertaken, including such phenomena as hacking, hacktivism or cyber-terrorism. Finally, an analysis of the most significant examples of competition and cooperation of countries in cyberspace has been conducted. On the one hand, the following events have been discussed: the situation in Estonia in April and May 2007, in Georgia in August 2008 and in Iran since 2010 (Stuxnet). On the other hand, the instances of cooperation between countries in that field were characterized on the basis of the following examples: The United Nations, The European Union, NATO and The African Union.

Miron Lakomy

Cyberespace en tant que nouvelle dimension de la rivalisation et coopération des États

Résumé

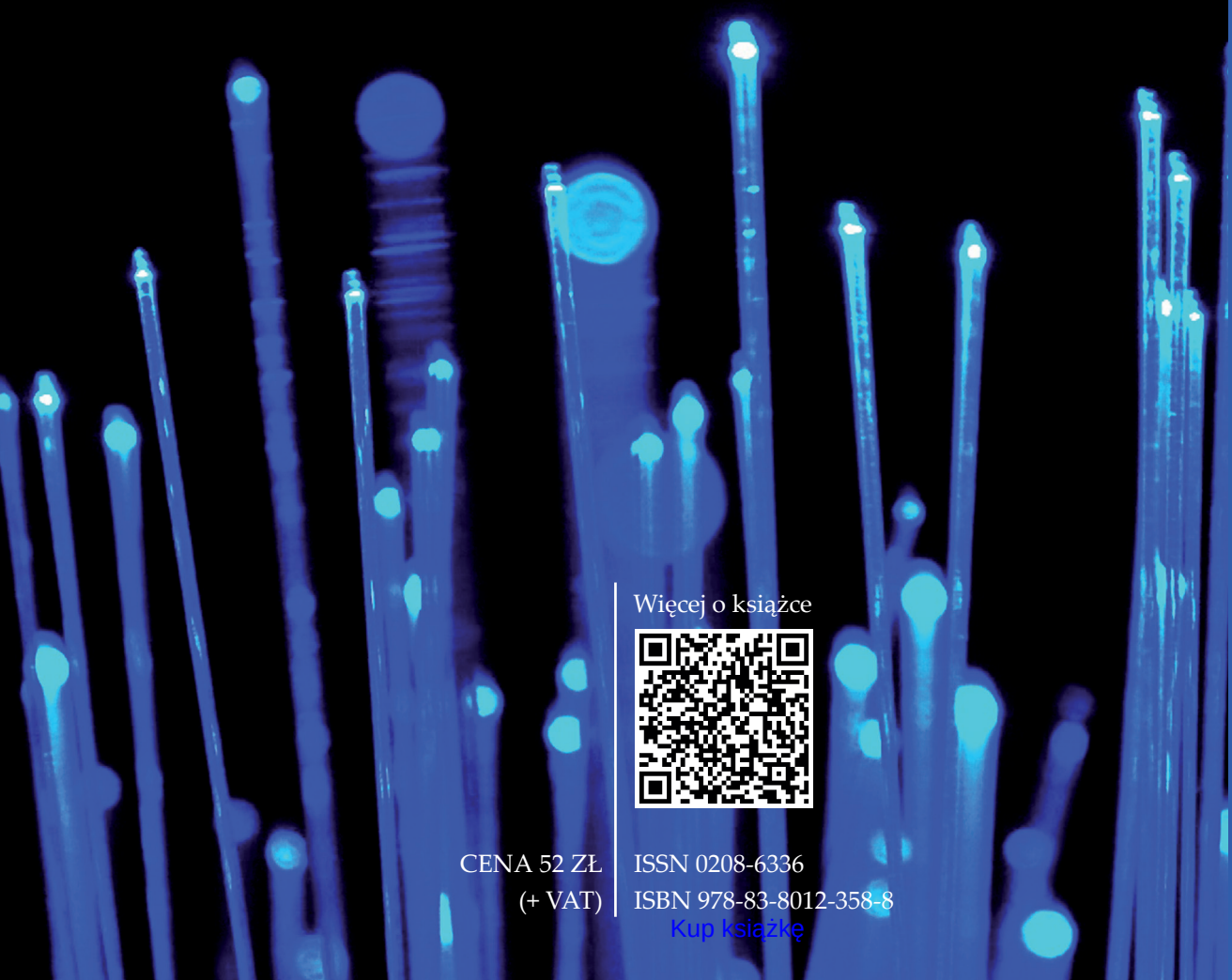
La révolution informatique qui s'est déclenchée pour de bon dans la seconde moitié du XXe siècle, à peine en quelques décennies a considérablement changé la physionomie du monde sur presque tous les plans possibles. Conformément aux prévisions d'une partie de déterministes technologiques, les procédés de l'application des ordinateurs au traitement des données et des informations ont vite envahi de nouveaux domaines de la vie des individus et de leur collectivité : de l'économie, en passant par l'enseignement, le divertissement, et allant jusqu'à la politique et l'armée. Étant donné ses traits les plus significatifs consistant à surmonter toutes sortes de limitations liées au traitement, tranfert et stockage d'informations, il a énormément servi à l'humanité. La naissance du cyberespace, nouveau domaine unique dans sa forme, en est devenue le symbole. Ses traits particuliers font que depuis des décennies, il détermine au point de plus en plus haut le fonctionnement des États et des sociétés tout en s'infiltrant dans l'administration des pays, l'infrastructure critique, le secteur du commerce ou encore dans les forces militaires. Leur dépendance croissante de TIC est devenue en même temps la cause de l'apparition de certaines tendances négatives dont on subit les conséquences dans le monde entier. L'universalité et le caractère global des technologies téléinformatiques ont suscité des changements capitaux dans le milieu de sécurité. En contribuant à la révolution dans les affaires militaires (RMA), les ordinateurs et leurs réseaux sont devenus parallèlement la source et la plateforme des phénomènes nuisibles qui, avec le temps, ont commencé à être perçus à travers le prisme des menaces pour la sécurité nationale et internationale. Différents sujets comme simples amateurs, hackers, hactivistes, cyberterroristes ou encore organisations criminelles, justement grâce au cyberespace, ont trouvé une possibilité potentielle de pénétrer même dans les éléments les plus actifs des systèmes nationaux de sécurité. Autrement dit, il est paradoxalement devenu une nouvelle dimension de sécurité dont le rôle augmente proportionnellement aux progrès des procédés liés justement à l'application des ordinateurs au traitement des données et des informations. Encore dans les années 1990, même les plus dangereuses attaques informatiques étaient le plus souvent traitées, au plus, comme un certain incon-

vénient pour l'administration centrale. Cependant, déjà deux décennies plus tard, leur ampleur est devenue si grande que l'on a commencé a y voir l'un des plus importants défis pour la stabilité de tout le système international.

Dans ce nouveau milieu qu'est le cyberespace, un sujet exceptionnel restent les pays qui, il n'y a pas très lontemps, ne portaient pas de grand intérêt à développer leurs propres capacités d'agir dans cette sphère. Cela a commencé à changer plus ou moins à la charnière des XX^{e} et XXI^{e} siècles où les bénéfices potentiels qui en résultaient ont été aperçus par les élites politiques à peine de quelques pays tels que les États-Unis, la Russie, la Chine ou Israël. D'une part, on a commencé à s'occuper au développement du potentiel technologique et celui d'experts ce qui a permis de se protéger plus efficacement contre les effractions informatiques. D'autre part, on a compris qu'une activité offensive dans l'espace téléinformatique pouvait devenir une arme favorable de la rivalisation et confrontation avec d'autres sujets dans le milieu international. Les qualités objectives de ce domaine comme anonymat facilement accessible, « agéographicité » et « aterritorialité » ou bien frais « d'accès » peu élevés le favorisaient encore. De surcroît, les ambiguïtés liées à l'interprétation des dispositions en vigueur du droit international et celle des mécanismes de la coopération politique et militaire ont dénoté l'utilité de ces instruments. En l'occurrence, les procurseurs ont réussi, en quelques années seulement, à créer des capacités avancées dans ce domaine qui ont pu théoriquement servir à réaliser des buts déterminés sur différents plans.

Dans ce contexte, la présente dissertation essaye d'examiner l'efficacité des moyens téléinformatiques comme instruments de la politique extérieure des États dans l'après-guerre froide. Au cours de l'analyse, tout en prenant en considération les aspects de la rivalisation ainsi que ceux de la coopération des gouvernements dans le cyberespace, on a eu recours aux éléments de la théorie de la politique étrangère. Dans la thèse, on a présenté avant tout l'essentiel et les étapes particulières de la révolution numérique qui a abouti à la formation de l'espace téléinformatique. Ensuite, on a décrit ses traits les plus significatifs aussi bien sur le plan technique que politologique. En prenant ces éléments comme point de départ, on a tenté d'établir une typologie simplifiée de menaces téléinformatiques pour la sécurité des États qui englobe les phénomènes tels que hacking, hactivisme et cyberterrorisme. Enfin, on a analysé les exemples les plus importants de la rivalisation et coopération des États dans le cyberespace. D'une part, on a traité, entre autres, les événements qui se sont déroulés en avril et en mai 2007 en Estonie, en août 2008 en Géorgie ou ceux en Iran à partir de 2010 (Stuxnet). D'autre part, on a décrit également les différents aspects de la coopération des États dans ce domaine à l'exemple entre autres de l'Organisation des Nations Unies, de l'Union européenne, de l'OTAN et de l'Union africaine.

Dr MIRON LAKOMY – doktor nauk humanistycznych w zakresie nauk o polityce (specjalność: stosunki międzynarodowe). Absolwent politologii Uniwersytetu Śląskiego. W semestrze zimowym 2006/2007 studiował także na Université Paris Sud XI we Francji. Adiunkt w Zakładzie Stosunków Międzynarodowych Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego. Jego zainteresowania badawcze obejmują zagadnienia związane z cyberbezpieczeństwem, uwarunkowaniami konfliktów zbrojnych, a także polityką zagraniczną Francji, Polski oraz Stanów Zjednoczonych. Opublikował dotąd 2 monografie, około 40 artykułów naukowych oraz współredagował 2 prace zbiorowe. Jest stypendystą University of Cambridge (program Corbridge Trust – 2011). W 2011 roku realizował również grant badawczy International Council for Canadian Studies – *The significance of cyberspace in Canadian security policy*. Wykładał we Włoszech (Universita Degli Studi di Napoli – 2011) oraz we Francji (Université de Nice Sophia Antipolis – 2013) w ramach programu Erasmus LLP. Jest członkiem Polskiego Towarzystwa Nauk Politycznych oraz Polskiego Towarzystwa Bezpieczeństwa Narodowego.



Więcej o książce

CENA 52 ZŁ (+ VAT)
ISSN 0208-6336
ISBN 978-83-8012-358-8

Kup książkę

MIRON LAKOMY

Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw