CBKE
e-BIULETYN

Doktryna Hakerów – mit czy rewolucja? Uwagi na temat natury informacji, entropii cyberprzestrzeni i postawy awangardy rewolucji postindustrialnej

mgr Adam Haręża

Zakład Prawa Administracyjnego, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

Ubiegłe stulecie, wraz ze swoją niebywale barwną i złożoną historią, cechowała dążność do radykalnych przeobrażeń o charakterze politycznym, gospodarczym i społecznym, których zarzewie powinno się upatrywać w procesach o proweniencji rewolucyjnej. Dotykały one różnorodnych sfer życia człowieka, niosąc ze sobą ogromne zmiany i wdrażając niespotykane dotąd formy organizacyjne. Fenomenem ubiegłego wieku jest jednak zjawisko (ruch), które dokonało w lawinowym tempie kompleksowej transformacji zbiorowości ludzkich, kreując w ostateczności tzw. „społeczeństwa informacyjne". Zastanawiające, że określane mianem rewolucji informatycznej – działania państw i jednostek – bywają nieomal nie zauważanymi procesami w ocenie podmiotów (osób), które stały się w istocie ich ostatecznym ogniwem (konsumentem).

Ogromny postęp technologiczny wprowadził zupełnie nową jakość bytu człowieka, na wskroś uzależnionego od dostępu, przetwarzania i gromadzenia informacji. Tempo przemian jest wprost proporcjonalne do dynamiki postępu. W urzędach, instytucjach, bankach, sklepach, Internecie – wszędzie operuje się informacją. Współczesny świat to przestrzeń cybernetyczna, w której informacja stanowi spoiwo między wolą i decyzją wykonawcy, a efektem elektronicznie wydanej dyspozycji.

Praca ludzi jest trwale zespolona i skoordynowana z funkcjonowaniem komputerów. W relacjach pomiędzy człowiekiem a maszyną można wyróżnić przynajmniej trzy szczególne przypadki symbiozy: maszyna zastępuje człowieka w określonych czynnościach poznawczych, uwalniając go do nich (np. czujniki, detektory rejestrujące zmienne parametry otoczenia), człowiek

konstruuje maszynę w celu wspomożenia własnych organicznych i ograniczonych zdolności poznawczych (np. mikroskop), wreszcie – maszyna poznaje więcej niż istota ludzka (sytuacja hipotetyczna zakładająca, że urządzenie, po zapoznaniu się z informacją początkową, rozpocznie wykorzystywanie jej dla własnego poznania, bez dalszego udziału człowieka)[1]. Symbioza człowieka z urządzeniami elektronicznymi wkrótce osiągnie kolejne stadium, w laboratoriach bowiem tworzone są prototypowe „organizmy - hybrydy", w których krzem i białko współpracują w przetwarzaniu informacji[2].

Konwergencja technologiczna, komputeryzacja, postęp cywilizacyjny i industrialny wyzwala nieuniknioną potrzebę refleksji prawno – filozoficznej, która choć w niewielkim stopniu pozwoli zaspokoić potrzebę badań i dyskursu dotykającego problematyki społeczeństwa informacyjnego nazywanego często telematycznym, sieciowym, postindustrialnym bądź postmodernistycznym[3].

Już z początkiem lat siedemdziesiątych D. Bell zaobserwował i opisał specyficzną transformację społeczeństwa, w wyniku której miała nastąpić „epoka postindustrialna", a w konsekwencji informacyjna[4]. Zjawisko ujmowane jako determinizm technologiczny (według D. Vincka) występuje w dwóch wersjach – autonomii rozwoju techniki oraz jako jej olbrzymi wpływ na życie społeczne[5]. Materialną i niezbędną zarazem infrastrukturą kształtującą „idealne globalne" medium jest Internet, będący w istocie ucieleśnieniem bytu informacji, która w opozycji do „ograniczonego" świata rzeczywistego konsekwentnie buduje alternatywną i niczym nie skrępowaną cyberprzestrzeń[6].

Problematyka związana z pojęciem społeczeństwa informacyjnego to obszar o niebywale zawiłej i zmiennej strukturze. Dodatkowo sytuację komplikuje brak powszechnie akceptowanej

[1] Pisze o tym: M. Hetmański, Internet jako maszyna cybernetyczna, [w:] R. Skubisz (red.), Internet 2000, Lublin 2000, s. 431 i nast.

[2] Naukowcom z Uniwersity of Calgary i Instytutu Maxa Plancka w Monachium udało się połączyć procesor krzemowy z komórkami nerwowymi w taki sposób, że informacje przepływają bezpośrednio z tkanki biologicznej do krzemu, a pozostawione w neuronach ślady pamięciowe mogą być odczytywane przez procesor. Szerzej na ten temat: W. Sadowski, Szok szybkości, „Polityka" (10 kwietnia), 2004, s. 86 – 87.

[3] Zob. P. J. Durka, Komputer. Internet. Cyfrowa rewolucja, PWN, Warszawa 2000.; A. M. Wilk, Polska wobec wyzwań społeczeństwa informacyjnego [w:] R. Skubisz (red.), Internet 2000, op. cit., s. 143 i nast.; A. Toffler, Trzecia fala, PAN, Warszawa 2001.; D. Bell, The Comming of Post – industrial Society, Basic Books, New York 1973.; M. Castells, The Rise of the Network Society, Blackwell, Oxford, 1996.; M. Castells, The information Age: Economy, Society and Culture, Blackwell, Oxford, 2000.

[4] D. Bell The Comming of Post – Industrial (…), [w:] F. Fakuyama, Wielki wstrząs. Natura ludzka a odbudowa porządku społecznego, Warszawa 2000, s. 13.

[5] D. Vinck, Sociologie des scientes, Armand Colin, Paris 1995, podaję za J. Kulpińska, Od społeczeństwa post – industrialnego do społeczeństwa informacyjnego – koncepcje i dyskusje, s. 2, publikacja jest dostępna w Internecie pod adresem: http://www.uci.agh.edu.pl/agh/dep/wnss/konferencje/doc.

[6] Wyraz „cyberprzestrzeń" pochodzi z książki „Neuromancer" napisanej w 1994r. przez W. Gibsona (symbolizowała futurystyczny komputer wraz ze swoim środowiskiem). Współcześnie termin ten zyskał sobie ogromną popularność i może oznaczać „wszystko", co posiada związek z Internetem i komputerem. W dalszej części artykułu postaram się na kanwie literatury nakreślić granice znaczeniowe „cyberprzestrzeni".

definicji społeczeństwa informacyjnego, jak i ustaleń dotyczących jej znaczenia oraz granic[7]. Nie chcąc zatem wkraczać na mielizny pojęciowe tych zagadnień, pominę ten aspekt w dalszej części rozważań.

Godnym podkreślenia jest fakt, że informacja przestaje być traktowana wyłącznie jako wiadomość z jej subiektywnymi konotacjami, stając się immanentnym kodem tkwiącym w każdej rzeczy, który wyjęty z niej tworzy „rzeczy samoistne", innymi słowy postrzegana jest tak, jak odrębny byt fizyczny[8]. Buduje swoją przestrzeń – świat, który podlega specyficznym i współcześnie cyfrowym zasadom. Nawet sztuka, będąc przyjemnością wizualną i abstrakcyjną, jest wysublimowanym zbiorem informacji. N. Wiener – „ojciec cybernetyki" nadał jej odrębny, autonomiczny status, czyniąc z niej trzeci elementarny składnik rzeczywistości, pisząc: „(...) Informacja jest informacją, nie zaś materią i nie energią (...)"[9].

Dlatego by ogarnąć i zrozumieć „naturę informacji" niezbędnym zabiegiem jest podjąć kwestie pojęciowe – trudne i kontrowersyjne, zważywszy, że autorzy prac związanych z dziedzinami teorii informacji lub nauk pokrewnych raczej stronią od konstruowania jednoznacznych definicji, uciekając się najczęściej do metod opisowych.

Przez informację można rozumieć wszelkie zalecenie, zezwolenie, zakaz, nakaz, każdy opis i sprawozdanie bądź instrukcje i wzorce działania, które mogą być wykorzystane do spowodowania określonego postępowania adresata tej informacji[10]. Niekiedy jest utożsamiana z pojęciem wiadomości, bez względu na formę i proklamowaną treść[11]. Informacja to też powiadomienie, zakomunikowanie, wiadomość, czy wskazówka w znaczeniu terminologicznym i potocznym[12]. Bywa, że termin ten dotyczy instytucji trudniących się udzielaniem wskazówek, porad, zaleceń, w zakresie swoich kompetencji i wiedzy.

Na gruncie cybernetyki, informacja (prócz wyżej przytoczonej koncepcji N. Wienera) jest także niejednolicie pojmowana. W ujęciu ogólnym – jako stan układów wyróżniony przez badacza spośród innych jego stanów (np. wybrany element ze zbioru komunikatów o normach lub

[7] Por. M. Goliński, Społeczeństwo informacyjne – problemy definicyjne i problemy pomiaru, publikacja jest dostępna w Internecie pod adresem: http:// pawel.k.webpark.pl/si/.

Prawdopodobnie jako pierwszy termin "społeczeństwo informacyjne" użył w 1963r. japoński publicysta Tadao Umesao w artykule poświęconym ewolucyjnej teorii społeczeństwa opartego na przetwarzaniu informacji. Japoński termin „johoka shakai" spopularyzował dziennik „Hoso Asahi". Szerzej na ten temat: T. Goban – Klas, P. Sienkiewicz, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Kraków 1999, s. 33.

[8] Por. A. J. Kościański, Społeczeństwo informacyjne: propozycje konceptualizacji, „kultura i społeczeństwo" nr 3, lipiec – wrzesień 1999.

[9] N. Wiener, Cybernetyka czyli sterowanie i komunikacja w zwierzęciu i maszynie, Warszawa 1971, s. 173.

[10] Piszą o tym: H. Greniewski, Cybernetyka niematematyczna, Warszawa 1969, s. 29, 206.; H. Greniewski, M. Kempisty, Cybernetyka z lotu ptaka, Warszawa 1963, s. 9 i nast.

[11] Por. J. Nowakowski, W. Sobczak, Teoria informacji, Warszawa 1978; W. Piróg, Zagadnienia informacji i dokumentacji naukowej, Warszawa 1978.

[12] Por. M. Szymczak (red.), Słownik języka polskiego PWN, Warszawa 1996, T. I.

zachowaniach prawnych)[13]. Natomiast w pojęciu szczegółowym, jako treść przekazywaną przez pewnego nadawcę, której człowiek lub urządzenie zbudowane przez człowieka jest odbiorcą będącym w stanie ją przyjąć i przetworzyć. Informacja staję się kategorią subiektywną, zależną od świadomości człowieka (lub zdolności percepcji automatu, nadanej przez człowieka), czy formy w jakiej się ją przekazuje (np. cenna dla nadawcy informacja zakomunikowana do adresata – cudzoziemca nie rozumiejącego języka nadawcy staje się bezużytecznym i niezrozumiałym zbiorem dźwięków, podobnie jak w przypadku wprowadzenia do maszyny matematycznej zakodowanej informacji w niezrozumiałym dla urządzenia języku)[14].

Oryginalną i ciekawą koncepcję cybernetyczną zaprezentował M. Mazur. Za informację uznał związek między stanami tego samego zbioru, przy jednoczesnej ścisłej odpowiedzialności między stanami zbioru obrazów, a stanami zbioru oryginałów, skutkującej powstaniem informacji identycznych w obydwu zbiorach[15]. Aby w pełni zrozumieć myśl autora, niezbędny jest drobny komentarz.

W otoczeniu człowieka zachodzą różne zmiany; społeczeństwo dowiaduje się o nich za pośrednictwem komunikatów złożonych z elementarnych sygnałów odczytywanych przez odpowiednie rejestratory, służące do kumulacji tych komunikatów w formie skojarzeń (będących z kolei reprezentacją gnostyczną powiązań zjawisk w otoczeniu)[16]. Zakładając, że społeczeństwo posiada pewną skończona liczbę rejestratorów odbierających sygnały z otoczenia, można przyjąć, że pomiędzy stanami zbioru oryginałów (zespół obiektów i stanów rzeczywistego świata „energomaterialnego"), a stanami zbioru obrazów (zespół oznakowań, jakie członkowie określonego społeczeństwa przyporządkowują odpowiednim elementom świata rzeczywistego) zachodzi odpowiedniość[17].

Niebywale trafną i kompleksową „naturę" informacji przedstawił M. Bazewicz. Autor w konkluzji stwierdził, że informacja jest pojęciem abstrakcyjnym, nie posiadającym wagi, nie zajmującym przestrzeni i nie możliwym do bezpośredniej obserwacji. Postrzegana jest bowiem wyłącznie poprzez pryzmat ludzkich zachowań i pracę, jest zaś określana przez powszechnie obserwowane i dostrzegalne genetyczne, biochemiczne i neurologiczne atrybuty[18].

Tymczasem z cyfrowego punktu widzenia informacja to jedynie przepływ energii (prądu elektrycznego), lub jego brak, pozwalający „urządzeniu" za pośrednictwem symboli (bitów) dokonać właściwej analizy „niematerialnych" i abstrakcyjnych danych. Zgodnie z teorią

[13] A. Malinowski, wstęp do badań cybernetycznych w prawoznawstwie, Warszawa 1977, s. 116 i nast.
[14] H. Rot, Podstawy cybernetyki i informatyki prawniczej, Wrocław 1983, s. 64 i nast.
[15] Pisze o tym: M. Mazur, Cybernetyczna teoria układów samodzielnych, Warszawa 1966, s. 37 i nast.
[16] J. Kossecki, Cybernetyka społeczna, Warszawa 1981, s. 163.
[17] Ibidem, s. 164 i nast.
[18] Por. M. Bazewicz, Wizja społeczeństwa ery komunikacji, informacji i wiedzy XXI wieku, Wrocław 2000, s. 182 i nast.

C. Shannona (w wielkim uproszczeniu) przy pomocy „bitu" można przekazać informację o dwóch różnych zdarzeniach (przyjmuje ona postacie : 0 i 1 jako dwa symbole)[19]. Koncepcja ta stała się podwaliną pod stworzenie uniwersalnego układu realizującego operacje na cyfrach binarnych (dwójkowych). Zalety takiego systemu sprawiły, że stał się on dominującym sposobem reprezentacji informacji w komputerach.

Na gruncie teorii informacji, zgodnie w klasyfikacją zaproponowaną przez W. Weaver'a, prócz poziomu analiz formalnych (pozwalających ustalić ilość informacji za pomocą konwencjonalnej jednostki miary, czyli wspomnianego bitu) można wskazać również poziom semantyczny i pragmatyczny[20]. W pierwszym znaczeniu informacja jest pojmowana jako treść przekazywana przez nadawcę jakiemuś odbiorcy w formie komunikatu, w drugim definicja kładzie nacisk na jej rolę przy oddziaływaniu na odbiorcę, biorąc pod uwagę możliwości percepcyjne adresata[21].

W tym kontekście wskazanym wydaje się refleksja nad pojęciami pozornie tożsamymi, taki jak: dane i informacja. Otóż przez dane należy rozumieć przedstawienie faktów, pojęć albo poleceń w ustalony sposób, który umożliwia ich przesyłanie, analizę lub przetwarzanie przez ludzi oraz w sposób zautomatyzowany (program komputerowy jest specjalną kategorią danych, podobnie jak notatki, obrazy, jeżeli są dostatecznie sformalizowane i wypełniają powyższą zasadę)[22]. Natomiast informacja to wywołany danymi efekt, zamierzony lub doświadczony przez ich użytkowników. Uzyskanie informacji, w tym informowanie innych, polega na posługiwaniu się danymi, które przybierają charakter subiektywny, ponieważ są silnie uzależnione od czynników społeczno – kulturowych oraz ekonomicznych[23]. Syntaktyka, semantyka i pragmatyka statuują strukturę informacji jako określony zbiór symboli, których znaczenie zawsze musimy ustalić w wyniku subiektywnej interpretacji[24].

Rozdźwięk między powyższymi pojęciami jest logicznie nieunikniony. Informacja nie może być wyłącznie zbiorem danych – surowym materiałem inkorporującym dane, czy ich surogatem. Lecz jest subiektywnym efektem ich interpretacji, opisującym określony stan rzeczywistości oraz usytuowanym w opozycji do neutralnych semantycznie danych (posiadanie dostępu do nich nie musi być adekwatne z zapoznaniem się z zawartą w nich treścią informacji).

[19] Pisze o tym: H. Rheingold, Narzędzia ułatwiające myślenie. Historia i przyszłość metod poszerzania możliwości umysłu, Warszawa 2003.
[20] Pisze o tym: J. Petzel, Informatyka prawnicza: zagadnienia teorii i praktyki, Warszawa 1999, s. 36 i nast.
[21] Ibidem, s. 37 wraz z podaną w przypisach literaturą.
[22] Podaję za: Recommendation of the Council of the OECD concerning Guidelines for the Security of Information Systems, OECD/GD (92) 10 Paris 1992.
[23] A. Adamski, Prawo karne komputerowe, Warszawa 2000, s. 38.
[24] Por. K. Dobrzeniecki, Prawo a etos cyberprzestrzeni, Toruń 2004, s. 16.

Przy tak obranych założeniach wydaje się, że myśl L. Brillouin'a traktująca informację jako zbiór danych nie wyraża w pełni funkcji oraz istoty informacji[25].

Częstokroć współczesne teorie informacji stawiają znak równości między informacją a nieprzewidywalnością (generującą systemy chaotyczne)[26]. Jeśli wiadomość nie wnosi nic nowego, czyli nie udziela odpowiedzi bez względu na rodzaj i materię pytania lub abstrakcyjnego zagadnienia, to nie zawiera informacji, która ze swojej istoty musi stanowić novum (czasami pojmowane subiektywnie) dla odbiorcy. Staje się swoiście traktowanym i nieuporządkowanym strukturalnie składnikiem wiedzy.

Informacja bywa także traktowana w kategoriach politycznych, czasami pro – społecznych, jeśli przyjąć jej relatywizm wobec korelatu władzy. Nie tylko hipotetycznie można traktować ją jako czynnik lub „nośnik" zagrożenia w sytuacji zapoznania się z jej treścią, a nawet potencjalnego „posiadania dostępu" do niej przez osoby niepowołane (nieupoważnione), niekompetentne albo nieodpowiedzialne. Osoba lub instytucja dysponująca informacjami wyjątkowymi, czyli przeznaczonymi jedynie dla określonych i prawnie wskazanego kręgu podmiotów, jest predestynowana do właściwego ich użytkowania. Dostępność do informacji jest uwarunkowana głównie jej wartością (cennością), natomiast jej różnicowanie dotyczy nie tylko treści, ile uwzględnia kategorie odbiorców, warunkując konieczność ochrony wyselekcjonowanej informacji[27].

Z wszelkich cech informacji wynika, że można pojmować jej naturę w sposób różnorodny. Każda definicja wyłania i eksponuje na swój sposób sens informacji. Jej istotą i funkcją zarazem jest pogłębianie ludzkiej wiedzy, doświadczenia i budowanie coraz to szerszego wyobrażenia o otaczającej nas rzeczywistości. Bez względu na fizyczny charakter wydobywania informacji (np. w sposób wzrokowy, słuchowy, smakowy), dziedzinę nauki czy właściwości metrologiczne (np. mierzalne – wiek, waga i niemierzalne – kolor, zawód)[28] jej rolą jest wzbogacenie ludzkiej myśli. Forma zaś uzależniona jest od poziomu naszej cywilizacji. Począwszy od przekazów werbalnych, następnie treści utrwalanych w kamieniu, poprzez wynalazek Gutenberga, aż do obecnego cyfrowego (nienamacalnego) przekazu informacji.

[25] L. Brillouin, Nauka a teoria informacji, Warszawa 1969, s. 17.
[26] W. Rowland, (autor wstępu do książki) D. de Kerckhove, Inteligencja otwarta, Warszawa 2001, s. 16.
[27] Współcześnie około 20 % informacji podlega ochronie, a w najbliższych latach wartość ta może wzrosnąć do przeszło 50%. Por. E. Kuriata, Wirusy komputerowe. Mechanizmy infekcji i środki ochrony, Wrocław 1999, s. 14.
[28] W. Sobczak, W. Malina, Metody selekcji informacji, Warszawa 1978, s. 9 i nast.

Na bazie poczynionych uwag, warto zastanowić się nad cechami znamiennymi współczesnych form komunikacji. Za kryterium egzemplifikacji przyjąć należy obecne właściwości i wpływ informacji na cywilizację ludzką w dobie XXI stulecia:[29]

a. jest stale gromadzona, przetwarzana, tworzona i udostępniana, w celu jej efektywnego wykorzystania i koordynowania procesów podejmowania decyzji;
b. jest integralnym i kardynalnym składnikiem wytwórczym, stanowiąc dużą część wartości dodanej większości dóbr i usług;
c. przyjęła niematerialną – cyfrową postać oraz jest przekazywana przy pomocy urządzeń teleinformatycznych;
d. jest pozbawiona ekskluzywnego charakteru w takim sensie, że może być powielana bez uszczuplania jej zasobów (czyniąc ją w pewien sposób niezniszczalną w trakcie konsumpcji, gdyż liczba informacji nie zmniejsza się w toku jej wykorzystania);
e. przybrała właściwości synergiczne (wartość sumy informacji jest większa niż suma jej elementów składowych, co bezpośrednio jest powiązane z pojęciem jakości informacji);
f. zasadniczo wpływa na współczesną organizację społeczeństwa, w tym jego instytucji;
g. powielenie informacji stało się wyjątkowo łatwe, tanie i szybkie, natomiast „kopia" przybiera charakter idealny, ponieważ nie różni się jakością od „oryginału";
h. informacja (zwłaszcza jej obieg) kształtuje świadomość oraz standardy nowoczesnego społeczeństwa;
i. pełni funkcję integracyjną w aspekcie społecznym, gospodarczym i politycznym;
j. stała się najcenniejszym „dobrem" XXI w., wymagając przedsięwzięcia wyjątkowych środków ostrożności, które zabezpieczą przed wszelką niepowołaną próbą ingerencji w jej integralność, dostępność i poufność.

[29] Szerzej na ten temat: e – Europe: An information society for all – An Action Plan to be presented in view of the Sevilla Europe Council, 21/22 June 2002r.; OECD 1999 – OECD Workshops on the Economics of the Information Society: A Synthesis of Policy Implications, OECD, Paris 1999.; e – Polska – Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 – 2006, Ministerstwo Infrastruktury (źródło: www.mi.gov.pl); e – Polska 2006 – Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce, Ministerstwo Infrastruktury (źródło: www.mi.gov.pl); e – Polska – Strategia informatyzacji Rzeczypospolitej Polskiej, Ministerstwo Nauki i Informatyzacji (źródło: http://www.kbn.pl); Proponowane kierunki rozwoju społeczeństwa informacyjnego w Polsce do 2020r., Ministerstwo Nauki i Informatyzacji (źródło: http://www.kbn.pl); Gazeta IT, 9 (17), 2003 (2 październik), Społeczeństwo informacyjne to też zjawisko prawne.; P. Mullan, Information Society: Frequency un – asked questions, (źródło: http://www.spiked - online); C. Shapiro, H. Varian, Information Rules: A Strategic Guide to the Network Economy, Harvard Business Scholl Press, 1998.; A. Lekka Kowalik, Ukryte założenia społeczeństwa informacyjnego [w:] T. Zasępa (red.) Internet – fenomen społeczeństwa informacyjnego, Częstochowa 2001.;A. M. Wilk, Polska wobec wyzwań społeczeństwa informacyjnego [w:] T. Zasępa (red.) Internet – fenomen społeczeństwa informacyjnego, Częstochowa 2001.; J. Kropiwnicki, Budowa cywilizacji informacyjnej jako filar długookresowej strategii dla Polski do roku 2025 [w:] T. Zasępa (red.) Internet – fenomen społeczeństwa informacyjnego, Częstochowa 2001.; T. Goban Klas, P. Sienkiewicz, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Kraków 1999.; Z. Topolewski, Komputerowe zabezpieczenie poufności informacji w zarządzaniu, Wrocław 2002.; J.J. Szymona, Wolność i własność w Internecie [w:] R. Skubisz (red.) Internet – problemy prawne, Lublin 1999.

Nie sposób przecenić roli informacji, która pełni wobec nowej formacji cywilizacyjnej. Nie można również pominąć Internetu będącego najważniejszym i najpopularniejszym medium gromadzącym „digitalną" informację[30].

Zespolenie informacji cyfrowej i ludzkiej percepcji kreuje własną, oryginalną i niespotykaną w dziejach ludzkości przestrzeń informacyjną, nazywaną często w literaturze cyberprzestrzenią. Uznawaną za niematerialną emanację Internetu, o niepowtarzalnym, chaotycznym, heterogenicznym i zdecentralizowanym charakterze, unikalnej specyfice umożliwiającej połączenia wszelkich tradycyjnych mediów, zapewniającą swobodną wymianę idei, informacji i myśli[31].

Globalna sieć zlikwidowała dotychczasowe przeszkody komunikacji międzyludzkiej. Pewne utrudnienia, które niegdyś mogły uniemożliwiać swobodę wymiany myśli pośród zbiorowości (np. granice państw, cenzura) dziś są już jedynie reliktem przeszłości. Pojęcie „globalnej wioski", które na trwałe wprowadził M. Mcluhan, wydaje się nad wyraz trafne, mając na uwadze zewnętrzne warunki wzajemnej komunikacji, jakie umożliwia współczesna technologia, koncentrująca w sieci olbrzymią ilość rozmówców oraz zmniejszająca dystans ujmowany w geograficznym wymiarze[32].

Architektura cyberprzestrzeni uzależniona wprawdzie od materialnych urządzeń, dzięki którym może być gromadzona, przesyłana i przetwarzana informacja jest niebywale podatna na formowanie, rekonfigurowanie, czy modyfikacje (np. technologiczne)[33]. Ustawiczne zmiany zachodzące w obrębie tego globalnego medium uniemożliwiają tym samym zarysowanie choćby orientacyjnych jego granic, nadając tej strukturze wymiar fraktalnej i amorficznej postaci[34]. Zdecentralizowana i samoregulująca się sieć służąca zasadniczo do wymiany danych nie jest w dodatku wzbogacona w żaden „organ zarządzający" lub o „podobnej instancji kontrolnej"[35]. Brak jest zatem ośrodka koordynującego całością, dbającego o ład i porządek w sieci, wyposażonego w kompetencje normodawcze.

---

[30] Internet rozwija się w zadziwiającym tempie, przerastając najśmielsze oczekiwania twórców. Pod koniec roku 2002 liczba osób posiadających dostęp do Internetu przekroczyła 600 milionów. W roku 2006 blisko 80% populacji Stanów Zjednoczonych będzie korzystać z Internetu przynajmniej raz w miesiącu (źródło: http://www.winter.pl), zaś globalna sieć skrywała w swych zbiorach blisko 500 miliardów dokumentów.

[31] Pisze o tym: K. Dobrzeniecki, Prawo a etos, op. cit., s. 20 i nast. Autor słusznie dokonał rozróżnienia cyberprzestrzeni od przestrzeni wirtualnej (por. s. 10).

[32] Pisze o tym: B. Borowik, R. Borowik, Przemiany świadomości kulturowej w dobie społeczeństwa informacyjnego, (źródło: http://www.uci.agh.edu.pl/agh/dep/wnss/konferencje/doc/).

[33] Por. K. Dobrzeniecki, Prawo a etos, op. cit., s. 11 i nast.

[34] Pisze o tym: J. Staniszewski, Internet : problemy bezpieczeństwa informacji, „Problemy kryminalistyki", 1997, nr 216, s. 81 i nast. (tłumaczenie z „Wired" 5. 04., s. 132 i 5.05., s. 58.).

[35] Por. A. Henschke, Internet jako narzędzie przestępstwa, „Problemy kryminalistyki", 2001, nr 231, s. 72. (tłumaczenie z „Kryminalistik" 2000, nr 4, s. 229 – 239).

Również prawo w sieci nabiera specyficznego znaczenia. Internet ujmowany *sensu largo* nie podlega prawom własności, ponieważ nikt nie jest jego właścicielem. Poszczególni użytkownicy składający się na cybernetyczną społeczność dysponują, posiadają i zarządzają zaledwie określonymi ogniwami (udziałami).

Wielu Internautów nie respektuje, bądź błędnie pojmuje obowiązujące (bez względu na dziedzinę) normy prawne[36]. Niektórzy są przekonani o potrzebie wyodrębnienia z założenia odmiennej sfery prawa, obecnej tylko w „specjalnej" przestrzeni (stworzenie zupełnie nowej kategorii), rządzącej się autonomicznymi regułami[37]. Niemniej koncepcjami bardziej pragmatycznymi są idee utworzenia międzynarodowego prawa kolizyjnego albo unifikacja prawa na szczeblu międzypaństwowym[38]. Nie podlega dyskusji, że dominującą rolę w tych procesach będzie odgrywało prawo międzynarodowe, które zapewne zostanie poddane próbie systemowych rozwiązań prawnych na niespotykaną dotąd skalę, poprzez stworzenie i ratyfikowanie konwencji będącej rodzajem konstytucji, wyposażonej w katalog podstawowych przepisów i procedur umożliwiających rozstrzyganie wszelkich wątpliwości i problemów związanych z zastosowaniem tego globalnego medium, wykorzystanie *per analogiam* już istniejących przepisów, bądź wielostronną regulację działań prowadzonych w Internecie[39].

Pomimo, iż w cyberprzestrzeni działają obecnie różne typy norm prawnych i pozaprawnych, które wzajemnie się uzupełniają, krzyżują, a niekiedy konkurują ze sobą (np. regulacje wewnętrzne obowiązujące w danym czasie i terytorium, przepisy prawa międzynarodowego prywatnego, zapisy zawarte w regulaminach sieciowych oraz zasady netykiety)[40], wciąż istnieją problemy natury interpretacyjnej.

Można zatem pokusić się o postawienie tezy, że Internet, a ściślej cyberprzestrzeń, była od początku swego istnienia obszarem zupełnie pozbawionym mechanizmów kontrolnych, barier oraz „realnych" metod kompleksowej ochrony. Jedynym prawdziwym ograniczeniem są możliwości percepcyjne człowieka[41]. Przepisy prawne przegrywają rywalizację z amorficzną postacią cyberprzestrzeni i to niekoniecznie w aspektach postępu technologicznego pozostawiającego w tyle regulacje normatywne, które utrwalone wieloraką tradycją i stworzone z myślą o przyszłych pokoleniach, nie ulegają takim szybkim przeobrażeniom oraz z racji swojej monolitycznej

[36] Por. W. Beliński, Jak łamie się prawo w Internecie, „Prawo i Życie", 1998, nr 23 – 24, s. 42.
[37] Za wzór wskazywano przestrzeń kosmiczną. Szerzej na ten temat: A. Adamski, Międzynarodowa kontrola cybeprzestępczości (w:) T. Zasępa (red) Internet i nowe technologie – ku społeczeństwu przyszłości, Częstochowa 2003, s. 521 i nast.
[38] Por. M. Świerczyński, Cyberprawo – mity i fakty, „Prawo i Życie", 2001, nr 27, s. 27.
[39] M. M. Kenig – Witkowska, Niektóre zagadnienia prawnomiędzynarodowej regulacji Internetu, „Państwo i Prawo", 2001, z.9, s. 57 i nast.
[40] J. Jabłońska – Bonca, Normy obowiązujące w cyberprzestrzeni, „Gdańskie studia prawnicze", 2000, Tom VII, s. 212 i nast.
[41] Por. J. Horoszkiewicz, Internet – strefa niekontrolowana, „Przegląd policyjny", 2001, nr 2 (62), s, 100 i nast.

struktury, nie ułatwiają swobodnego dostosowania do standardów, jakie wymaga mobilne (cywilizacyjnie) społeczeństwo, kreujące nowe wzory postępowania[42].

Nieokiełznana cyberprzestrzeń jest wyzwaniem dla ludzkich aspiracji, to Internauci (motywy, jakimi kierują się w swych sieciowych poczynaniach) kształtują jej treść i wizerunek[43]. Braku barier nie powinno poczytywać się jako przyzwolenie do anarchii i rezerwatu patologii, lecz upatrywać w tej wspaniałej na swój sposób konstrukcji współczesnego azylu.

W istocie Internet może być rozważany w kontekście szeroko pojmowanych tendencji liberalnych. Paradoksalnie elastyczność architektury sieci, jak i niemożność objęcia jej we władanie, bądź wdrożenia w życie totalnego nadzoru, zabezpiecza jej użytkowników przed niepowołanymi lub zbyt dalece posuniętymi działaniami państw (nie wykluczając jednostek) prowadzącymi do ograniczenia podstawowych praw. Cechy gatunkowe Internetu zabezpieczają (gwarantując tym samym) równość wszystkich Internatów, tolerancję i brak cenzury, czy swobodę wyrażania i krzewienia idei wolnościowych (szeroko pojmowanych). Informacja zawsze może w gąszczu globalnej pajęczyny „wybrać" drogę awaryjną, jeżeli jedna z „części składowych zostałaby usunięta"[44]. Ponadto człowiek korzystający z Internetu nabywa niebagatelną i niczym nieskrępowaną możliwość (wolność) kształtowania własnej osobowości[45].

Rzeczywistość zdecydowanie nie przystaje do tak projektowanego (idealistycznego) modelu zachowania (wykorzystania sieci). Więcej, odbiega od ogólnych paradygmatów właściwego postępowania. Przestępczość komputerowa i internetowa, cyberpiractwo, komercjalizacja Internetu, naruszanie dóbr osobistych i niejednokrotnie danych osobowych, swobodny dostęp do treści pornograficznych, stowarzyszeń propagujących totalitarną formę władzy, wreszcie bezideowe i często bezcelowe próby sparaliżowania Internetu (np. poprzez ataki wirusów) jedynie pogłębiają poczucie niebezpieczeństwa i bezradności Internautów[46]. Brytyjski Home Office alarmuje o eksplozji przestępczości wykorzystującej elektroniczną transmisję danych[47].

---

[42] Por. T. Kaczmarek, Polskie prawo karne wobec przestępczości komputerowej (w:) L. Bogunia (red.) „Nowa kodyfikacja prawa karnego", 2001, T. VIII, s. 57.

[43] Mimo wszelkich obostrzeń, starań i przeszkód ze strony władz, licząca ponad 60 milionów armia użytkowników Internetu stała się nieoczekiwanie jedną z najważniejszych sił w demokratyzacji Chin. Szerzej na ten temat: A. Burchard, Prawo wymaga jeszcze ofiar, „Polityka" nr 42 (2423). Na temat historii Internetu zob.: A. Baran, W pajęczynie Internetu: przewodnik dla początkujących, Lublin 1996.;T. Bienias, Internet, Kraków 1998; B. Leś, ABC... Internetu, Kraków 1998.

[44] Por. H. Rheingold, The virtual community: Homesteading on the electronic frontier, Reading, MA; Addison – Wesley, 1993, s. 7.

[45] Por. B. Wojciechowski, Sieć na człowieka, „Wprost" 1999, (9 maja), s 73.

[46] Tytułem przykładu można wskazać ataki tzw. „cyberterrorystów", którzy pod koniec 2002r. niemal nie spowodowali unieruchomienia całego Internetu. Szerzej na ten temat: M. Adamczyk, M. Kowalczyk, Bomba Internatowa, „Wprost" 2002 (3 listopada), s. 55 – 58.

Warto dodać, że laboratorium wirusów komputerowych o światowej renomie – Sophos wykrywa codziennie średnio 25 wirusów. Por. www.hacking.pl

[47] Pisze o tym: P. Dąbek, Raj przefiltrowany, „Chip", 2001 (21 marzec), s. 87 i nast.

Bezpieczeństwo systemów i sieci komputerowych jest bardzo poważnie nadwątlone. Cyfrowa przestrzeń teleinformatyczna jest wymarzonym środowiskiem kryminogennym[48]. W konsekwencji globalna sieć kojarzy się „potencjalnym" oraz „obecnym" użytkownikom z przestrzenią permanentnego zagrożenia, beztroskim łamaniem prawa, bądź nagminnym naruszaniem prywatności.

Wszystkie wyżej wskazane czynności niezgodne nie tylko z literą prawa, ale przede wszystkim z „duchem Internetu", nie wymagają dla swej skuteczności szczególnej wiedzy czy umiejętności[49]. Natomiast wdrażając i wzmagając chaos, zdecydowanie przyśpieszają procesy entropii cyberprzestrzeni. Konsekwencje mogą być katastrofalne.

W obliczu pogrążania się globalnej sieci w „otchłani" bezprawia oraz ignorancji, liczni naukowcy i publicyści zaangażowani w pomyślny rozwój tego medium starają się przeciwdziałać tym pejoratywnym zjawiskom i zachowaniom. Niektórzy zaś przeciwnie, wieszczą zmierzch, a nierzadko autodestrukcję Internetu[50]. Opisując ciemną stronę sieci nie sposób pominąć „operacji" dokonywanych przez rządy państw z różnych powodów, a także w imię rozmaitych idei. W ostateczności pogłębia się ingerencja owych podmiotów, doprowadzając czasami wpływy poszczególnych podmiotów do granic absurdu. Bowiem wirtualny teatr wojny informatycznej oraz bogaty arsenał technik komputerowych sprawił, że „pole zmagań" walczących objął swym zasięgiem wszelkie pola cyfrowej eksploatacji[51]. Sabotaż komputerowy, wirusy, urządzenia i oprogramowanie służące do podsłuchu, bomby mikrofalowe, broń magnetyczna to zaledwie początek ogromnej listy działań „wojny elektronicznej"[52], powiązanej ze szpiegostwem komputerowym[53], rywalizacją o elektroniczną hegemonię wywiadów państw na całym globie[54] oraz cyberterroryzmem[55].

Internet w takim kształcie zatraca swoje „naturalne" walory, stwarzając „przestrzeń" nieprzyjazną dla człowieka. Nie można traktować Internetu w kategorii panaceum na wszelkie problemy trapiące ludzkość, ponieważ „(...) sprawniejsza komunikacja, elektroniczne programy

[48] B. Hołyst, Kryminalistyka, Warszawa 2000, s. 285 i nast.
[49] Por. W. Krusiński, M. Ścibior, Plusy i wirusy, „Polityka" 2004 (30 października), s. 88 – 91.
[50] Fiński profesor Hannu H. Kari jest przekonany, że Internet w swym obecnym kształcie ma szanse przetrwać jedynie kilka lat. Sieć jest bowiem przeładowana „spamem", atakowana wirusami i innymi programami mającymi na celu jedynie destrukcję. Sieć zaczyna pękać w szwach również od reklam. Coraz częściej wspomina się o konieczności kontroli internetowych witryn. Szerzej na ten temat: T. Walat, Zaciskanie sieci, „Polityka", 2004 (20 marca), s. 60 – 61.; M. Rabij, Cel:Internauta, „Newsweek", 2004 (27 czerwca), s. 54.
[51] Information warfare; I-War, C4I, Cyberwar – istnieje wiele terminów na określenie zjawiska. Przykładowe strony internetowe opisujące problematykę można odnaleźć pod adresem: http://www.psycom.net/iwar.1.html http://www.informationwar.org/
[52] Wojna informatyczna generuje przy okazji ogromne wydatki. Tylko w USA wydaje się na ten cel od 100 do 300 miliardów dolarów rocznie. Por. B. Hołyst, Psychologia kryminalistyczna, Warszawa 2004, s. 862.
[53] Pisze o tym: J. Mc Namara, Arkana szpiegostwa komputerowego, Gliwice 2004.
[54] Pisze o tym: J. Guisnel, Wojny w cyberprzestrzeni, Kraków 1998.
[55] Pisze o tym: M. J. Weber, Naruszanie prywatności. Wielki brat i korporacyjni hakerzy, Warszawa 2004, s. 118 i nast.; D. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Toll for Influencing Foregin Policy (http://www.terrorism.com); A. Adamski, Cyberterroryzm (http://www.low.uni.torun.pl/komp-lex.pyblikacje).

oraz (...)dostęp do wszechświata informacji nie rozwiąże naszych problemów (...)"[56]. Spełnia on jednak bardzo ważne funkcje w społeczeństwie informacyjnym, przede wszystkim z uwagi na szybkość, łatwość i różnorodność reprezentowanej w tym medium wiedzy oraz zasobów. Tak więc – nasza cywilizacja już „pochłonęła" Internet oraz w pewien sposób uzależniła swój los od istnienia globalnej sieci, która stworzyła miejsce dla swobodnego rozwoju „cyfrowej informacji" (cyberprzestrzeni).

Rodzi się zatem podstawowe pytanie: kto lub co będzie w stanie powstrzymać, albo bynajmniej ograniczyć, postępujący proces entropii cyberprzestrzeni, prowadzący niechybnie w stronę destabilizacji i dezinformacji Internetu, czyli jego destrukcji? Wydaje się, że w takim otoczeniu grupą stanowiącą niezłomny filar i gwarant bytu cyfrowej przestrzeni są nad wyraz uzdolnieni ludzi, których zwykło się określać mianem hakerów[57]. Zaistnieli jako awangarda rewolucji postindustrialnej i trwają na swym piedestale nadal. Ich postawa, filozofia oraz dokonania zorientowane na pomyślny rozwój informatycznej infrastruktury oraz społeczeństw bazujących na informacji są nie tylko entuzjastycznym prognostykiem rozwoju cywilizacji ludzkiej w swym obecnym kształcie. Lecz paradoksalnie, stanowią gwarant względnej stabilizacji i postępu.

Termin „haker" jest pojęciem najbardziej wieloznacznym w całej publicystyce i nauce powiązanej sensu largo z komputerami oraz Internetem. Na taki stan rzeczy wpływają różnorakie czynniki, spośród których dominujące znaczenie przypadło mass-madiom i coraz bogatszej literaturze kreującej przeróżne oblicza hakerów[58]. Nie sposób przeoczyć wyraźną ewolucję

[56] C. Stoll, Krzemowe remedium. Garść rozważań na temat infostrady, Poznań 2000, s. 63.

[57] Uznałem za stosowne stworzyć neologizm będący polskim odpowiednikiem terminu hacker, hacking i jego odmian (np. craker – cracking).

[58] Zob.: 131ah, R. Rogers, J. Beale, J. Grand, Fyodor, FX, P. Craig, T. Mullen (Theor), T. Parker, Hakerzy atakują. Jak podbić kontynent, Gliwice 2004; Dr – K, Podręcznik hakera. Wszystko w hakerstwie w dobie Internetu, Warszawa 2002; K. Mitnick, W. Simon, Sztuka podstępu. Łamałem ludzi nie hasła, Gliwice, 2002; J. Mrugalski, ABC ochrony komputera przed atakami hakera, Gliwice 2003; D. Verton, Pamiętniki hakerów. Fascynująca opowieść o nastoletnich hakerach, Gliwice, 2002; D. Doroziński, Hakerzy. Technoanarchiści cyberprzestrzeni, Gliwice, 2001; R. Flickenger, Serwer linuksowy okiem hakera, Warszawa 2003; W. Wang, Internet, hakerzy, wirusy..., Warszawa 2001;A. Dudek, Nie tylko wirusy. Hacking, cracking,bezpieczeństwo Interentu, Gliwice 1998; O. Bowcott, S. Hamilton, Hackerzy – włamywacze i komputery, Warszawa 1993; A. Warhole, Atak z Internetu, Warszawa 1999; L. Klander, Hacker proof, czyli jak się bronić przed intruzami, Warszawa 1998; K. Mendia, CH. Proise, Hakerom śmierć!, Warszawa 2002; A. Fadia, Etyczny hacking. Nieoficjalny przewodnik, Warszawa 2003; J. Scambray, S. McClure, G. Kurtz, Hakerzy – cała prawda. Sekrety zabezpieczeń sieci komputerowych, Warszawa 2001; J. Scambray, S. McClure, Hakerzy w Windows 2000, Warszawa 2002; J. Scambray, M. Shema, Hakerzy. Aplikacje webowe, Warszawa 2002; G. Kurtz, B. Hatch, J. Lee, Hakerzy w Linuksie. Sekrety zabezpieczeń sieci komputerowych, Warszawa 2003; J. Chirillo, Leksykon hackingu, Gliwice 2003; M. Schiffman, Hakerzy! – wyzwanie, Warszawa 2002; V. Ahuja, Bezpieczeństwo w sieciach, Warszawa 1997; M. Maj, K. Silicki, Klasyfikacja i terminologia incydentów naruszających bezpieczeństwo sieci [w:] R. Skubisz (red.), Internet 2000, prawo, ekonomia, kultura, Lublin 2000; B. Fischer, Hackpospolita Polska, „Prawo i Życie", 1997, nr 24; J. Borowski, Zatrudnię hackera, „Wprost" z 21 I 2001; K. Król, Inwazja spamerów, „Wprost" z 20 II 2000; J. Bochenek, Szpieg online, „Wprost" z 14 marca 1999; N. Socha, Bezprzewodowi hakerzy, „Wprost" z 27 X 2002; E. Bendyk, Haki na hakerów, „Wprost" z 29 marca 2003; E. Bendyk, Pojedynek hakerów, „Polityka" z 13 września 2003; K. Król, Czernobyl w cyberprzestrzeni, „Wprost" z 9 maja 1999; M. Szokoło, Wirtualny włamywacz, „Wprost" z 8 sierpnia 1999; B. Miś, Cyberwłamywacze, „Wiedza i Życie", 2001, nr 5; J. Kuraś, Hacker – bezmyślny wandal, magazyn komputerowy „Chip", grudzień 1999; J. Żmudziński, Hacking in Poland ' 98, „Chip", czerwiec 1998; M. Staniewicz, Mitnick i inni, „Chip", marzec 2003; M. Bugajska, (Nie)spokojny sen, „Chip", styczeń 2002; M. Nowak, Uchylanie żelaznej kurtyny, „Chip", październik 2002; M. Zimnicki, Manipulatorzy umysłów, czyli inżynieria społeczna w praktyce, „Internet", lipiec 2003; M. Zimnicki, Bezpieczeństwo danych w Internecie, „Internet", grudzień 2000; M. Hołyński, Hakerzy wszystkich krajów łączcie się!, magazyn komputerowy „Enter", sierpień 2000; D. Kucharczyk, PC pod ochroną, „Enter", luty 2002; M. Kamfora, Kult hakingu, „Enter", listopad 1999.; S. Szczepański, Hakerzy – ciemna strona informatyki, Pckurier nr 6/1999; A. Czarnowski, Noc

koncepcyjną tego pojęcia, jaka nastąpiła na przełomie lat. Z biegiem czasu przybrała postać dość różnorodnej i bez mała erudycyjnej myśli. Dlatego zagadnienie „hakerstwa" występuje w tak wieloznacznym kontekście.

Liczne witryny internetowe, zarówno polskie jak i zagraniczne, nie rozwiązują problemu[59]. Przeciwnie, ich mnogość i zawartość badana ze względu na treść, jak i „oprogramowanie" udostępnione dla każdego użytkownika Internetu, dodatkowo komplikuje omawianą materię, dołączając im wrogą etykietę i czyniąc z nich złowieszczych „cybermagów" mogących dowolnie manipulować sprzętem komputerowym. Utarła się bowiem w opinii publicznej wizja hakera - cyberprzestępcy, człowieka który uszkadza systemy, atakuje wirusami, jest aspołeczny i zawsze przysposobiony na wyrządzenie możliwie największych szkód.

Obecne rozpoznanie środowiska wynika w dużej mierze z inwersji znaczeniowej oraz „patologicznej postawy" osób samozwańczo okrzykniętych mianem hakera. Wielu młodych ludzi, aby zaistnieć bądź zaspokoić swoje ambicje, jest skłonnych popełniać czyny wypełniające ustawowe znamiona przestępstwa[60]. Najczęściej są to „drobne i pospolite" czynności naruszające literę prawa, które wynikają bardziej z przekory i braku fachowej wiedzy, aniżeli z chęci wyrządzenia szkody, lecz pozostawiają złe wrażenia i budują błędne wyobrażenie o całej społeczności. Na ogólny wizerunek tego grona mają wpływ również „nieudolni uzurpatorzy" kalający prawdziwy „kunszt hakerski", który w swej nieskazitelnej i pierwotnej odmianie

---

hakerów, Pckurier nr 12/1999; A. Skura, Zmiana warty. Linux kontra UNIX, Pckurier nr 7/2003; M. Maj, Zdążyć przed intruzem, Pckurier nr 8/2002; M. Rzewuski, Psychologia hakera, Pckurier nr 3/2003; B. Miś, Cyberwłamywacze, „Wiedza i Życie" nr 05/2001; P. Bulski, Sieci bezprzewodowe łatwym łupem dla hakerów - wyniki badań RSA Security : http://www.pclab.pl/ (18 lutego 2003); P. Bulski, Dobry haker Mitnick, źródło: http://www.pclab.pl/ (11 marzec 2003);P. A. Taylor, Hackers. Crime in the digital sublime, London and New York, First published 1999; K. Hafner, J. Markoff, Cyberpunk. Outlaws and hackers on the computer frontier, New York 1995; E. Nuwere, D. Chanoff, Hacker Cracker: A Journey from the Mean Streets of Brokkllyn to the Frontiers of Cyberspace, New York 2002; S. Levy, Hackers: Heroes of the Computer Revolution, Penguin, 2001.

[59] Poniżej zostaną przedstawione jedynie wybrane witryny internetowe poświęcone tematyce hakerskiej:
http://hacking.pl/topic.php?op=Hackers
http://cybercore.republika.pl/
http://www.underground.org.pl/
http://o2.pl/internet_komputery/hacking/
http://underground.zone.prv.pl/
http://search.wired.com/wired/default.asp?query=hackers
http://www.2600.com/
http://www.haker.com/
http://www.hackerz.org/
http://www.genocide2600.com/
http://www.antionline.com/
http://www.checksum.org/
http://www.hack3r.com/
http://www.10pht.com/
http://www.defcon.org/

[60] Badania wykazały, że wraz z przenikaniem technik informatycznych do nowych sfer naszej egzystencji, komputer może być zastosowany przez sprawców do wszystkich form i rodzajów przestępstw, co oznacza, że został obalony „mit" homogenicznej z punktu widzenia fenomenologii – cybeprzestępczości. Pisze o tym: U. Sieber, The International Handbook on Computer Crime. Computer - Related Economic Crime and the Infrigement of Privacy, John Wiley and Sons, Chichester - New York - Brisbone - Toronto - Singapure 1986, s. 26 i nast.

sąsiadował z nauką, geniuszem i artyzmem, stroniąc od rzemiosła czy wandalizmu. Wprawdzie nie można prawić o upadku idei, ale na pewno o jej błyskawicznie postępującej wulgaryzacji.

Poza tym hakerem nie jest osoba, która przy pomocy komputera (bądź innych elektronicznych urządzeń), dysponując przy tym odpowiednią wiedzą dokonuje przestępstwa. Ta kategoria wykracza poza ramy pojęciowe, ponieważ dotyczy podmiotów, których wyłącznym zamiarem jest chęć popełnienia czynu zabronionego, zazwyczaj powiązanego z możliwością osiągnięcia konkretnej i wymiernej korzyści majątkowej. Haker nie kradnie, nie niszczy, nie naraża na szkody. Odmienny jest zatem jego cel, motywacja i skutek od sfery intencjonalnej przestępców.

Pojęcie cyberprzestępcy, cyberterrorysty, cyberwłamywacza nie powinno być zatem tożsame z pojęciem hakera. Podobnie jak nietrafiony jest podział na „dobrego i złego hakera", stwarzający semantyczny dysonans i potęgujący „mętne" zrozumienie istoty rzeczy. Przynależność do „gremium hakerów" nie jest przecież uzależniona od aspektów aksjologicznych, natomiast ocena czynów badana poprzez pryzmat przestępstw komputerowych należy do wymiaru sprawiedliwości.

Priorytetowym zadaniem wydaje się wskazanie odpowiedzi: Kim jest haker? Mało pomocne są wyjaśnienia zawarte w słownikach. Oznaczają fanatyka komputerowego, zazwyczaj takiego, który poprzez komputer włamuje się do systemów operacyjnych różnorodnych podmiotów (firm, korporacji, organizacji, a także instytucji rządowych). Poprzez umiejętne manipulowanie programem komputerowym uzyskuje nieuprawniony dostęp do cudzych danych[61]. Przejawia zainteresowania i biegłość w zagadnieniach technicznych oraz fascynuje się rozwiązywaniem trudnych problemów, wynikających wielokroć z ograniczeń, jakie stawia oprogramowanie bądź urządzenie komputerowe. W żargonie informatycznym to międzynarodowe określenie osoby, która włamuje się do systemów i sieci komputerowych, pokonuje zabezpieczenia w postaci kodów i haseł broniących dostępu do zgromadzonej tam i przechowywanej bądź przetwarzanej informacji[62].

Z prawnego punktu widzenia „modus operandi" hakerów nie ogranicza się jedynie do przełamywania zabezpieczeń obejmując, bogate spektrum technik[63], dzięki którym infiltrują zawartość systemów komputerowych, usuwają lub modyfikują dane zgromadzone na twardych

[61] Por. słowniki: Collinsa i Longmana.
[62] J. W. Wójcik, Hacking!, „Prawo i Życie", 1998, nr 36 , s.14.
[63] Wybrane metody stosowane przy popełnianiu przestępstw komputerowych to: Koń trojański; Wirus; Bomba logiczna; Spoofing; Robak komputerowy; Metoda Salami; Blokowanie serwerów; Poszukiwanie luk w systemie; Superzapping; Back doors; Piggybacking; Network snooping; Przechwytywanie haseł; Expliot; Buffer overflow; Denial of service; Distributed Denial of servise (zaawansowana metoda Denial of service); Ping of death; Social Engineering.

dyskach, czy uniemożliwiają funkcjonowanie warstwy sprzętowej, czasami nawet bez konieczności forsowania zabezpieczeń chroniących przed ingerencją osób niepowołanych[64].

Wszystkie wcześniej przedstawione definicje po części przybliżają, ale nie obrazują istoty zagadnienia. Składają się na swego rodzaju pojęciową „schizofrenię". Z jednej strony są dalekie od prawdy, jeśli mamy na myśli „prawdziwego hakera", z drugiej zaś, poprzez symboliczny charakter tego terminu, można wypreparować rozmaite funkcje, jakie spełnia on w dobie społeczeństwa informacyjnego, zwłaszcza w odniesieniu do zabiegów klasyfikacyjnych (np. systematyka incydentów naruszających bezpieczeństwo sieci). Wieloznaczność terminologiczna może w pewnym sensie przyczynić się do bliższego poznania rzeczywistości. Niemniej topologia hakera, spychająca go do rangi „persona non grata", widoczna na co dzień w nagłówkach prasowych, obecna w wiadomościach telewizyjnych i potęgowana w Internecie, jest niepożądana i nierzetelna.

Trafnie ową kwestię podejmuje autor „Jargon file" - E.S. Raymond w publikacji internetowej na temat :"Jak zostać hakerem"[65]. Wyłożył w tym lakonicznym artykule esencję filozofi, która nie dotyczy – co bywa zaskakujące - wyłącznie środowiska programistów. Każdy bowiem w dowolne wybranej dziedzinie może przybrać postawę hakera, właściwie wykorzystując ją na najwyższych poziomach nauki czy sztuki. Natura hakera jest niezależna od szczególnego przedmiotu jego pracy[66].

Aby stać się hakerem (intelektualnie i emocjonalnie) nieodzowne jest przybranie należnej postawy. Została ona nakreślona poprzez „sztywne" zasady, którym każdy haker jest zobligowany hołdować i wcielać w życie. Tylko poprzez sumienną ich realizację można nabyć niezbędne umiejętności i przynależne tylko hakerom podejście do otaczającego świata, wyrażone w ich uniwersalnych prawidłach, takich jak:[67]

a. Świat jest pełen fascynujących problemów czekających na rozwiązanie;
b. Żaden problem nie powinien być rozwiązywany dwa razy;
c. Nuda i harówka są złe;
d. Wolność jest dobra;
e. Podejście nie jest substytutem kompetencji.

[64] Abstrahując od kwestii, że w praktyce złamanie hasła odbywa się często w sposób zautomatyzowany i haker jest powiadomiony wyłącznie o przełamaniu zabezpieczenia, nie zaś o jego treści, która nadal paradoksalnie może pozostawać utajniona.
[65] Tekst jest dostępny w języku polskim na stronie internetowej o następującym adresie: http://www.h4ck3r.prv.pl/hacker-howto.pl.html. Natomiast oryginalna i aktualna wersja angielska znajduje się: http://www.tuxedo.org/~esr/faqs/hacker-howto.html. Por. też http://www.catb.org/jargon/ (v.4.4.7). Stanowisko autora jest również podzielane na niektórych grupach dyskusyjnych.
[66] Lecz w dalszej części będę koncentrował się nad tradycyjnym pojmowaniem hakerów – informatyków.
[67] Por. http://www.h4ck3r.prv.pl/hacker-howto.pl.html.

Jeśli dodamy katalog niezbędnych umiejętności, jakie musi posiąść haker (np.: opanowanie sztuki programowania, najlepiej w różnych językach; administrowanie jednym z wybranych Unixów[68] z Open Source[69]; używanie i kreowanie stron WWW[70] w HTML'u[71]) oraz zadania, jakim musi sprostać (pisanie, testowanie i usuwanie błędów w programach o udostępnionym kodzie źródłowym, publikowanie użytecznych informacji, utrzymywanie informatyczno - hakerskiej infrastruktury w sprawności, a także propagowanie w pozytywnym sensie tej kultury), to wówczas możemy nakreślić w miarę obiektywny wizerunek tego środowiska.

Z całą pewnością haker to badacz złakniony nowych problemów, gotowy do wszelkich wyrzeczeń i skłonny podporządkować swoje życie zdobywaniu nowych zdolności, wiedzy i ćwiczeniu inteligencji. Ktoś, kto znajduje przyjemność w podejmowaniu intelektualnych wyzwań, jakie niosą ze sobą przezwyciężanie lub omijanie napotykanych ograniczeń, z entuzjazmem (graniczącym wręcz z obsesją) oddając się programowaniu.

Rozwiązywanie trudności i pokonywanie kolejnych przeszkód jest jego egzystencjalnym imperatywem. Dostrzegając wielość pytań pozostawionych bez odpowiedzi i w obawie przed upływem cennego czasu na rozważaniu już rozstrzygniętych kwestii, hakerzy mają moralny obowiązek dzielić się zdobytymi informacjami. W ten sposób wykluczają odtwórczość i unikają syzyfowej pracy, potęgując swe wysiłki na rozwiązywaniu nowych zagadnień. Taka postawa implikuje dążność do samodoskonalenia, eliminując tym samym rutynę prowadzącą do schematyczności. W tym sensie haker jest na wskroś wolnym indywidualistą, który potrafi jednocześnie współpracować z innymi hakerami i to nie tylko z racji samej przynależności do „wspólnoty", lecz poprzez realizację i wyznawanie tych samych reguł.

Hakerzy, obawiając się utraty swej wyznaczonej jasnymi kryteriami sfery indyferentnej, dzięki której mogą się stale rozwijać i rozwiązywać fascynujące ich problemy, są z natury zagorzałymi przeciwnikami wszelkiego autorytaryzmu. Wychodzą z założenia, iż omnipotencja władzy zawsze w konsekwencji zniewoli ich najcenniejszy „dar", czyli wolność i kreatywność rozumowania. Upatrują w takich rządach zagrożenia niczym nieskrępowanego bytu oraz postawy separującej od reszty społeczeństwa (co nie zawsze musi oznaczać „dziwacznego odludka"

[68] UNIX, system operacyjny przeznaczony głównie dla komputerów pełniących rolę serwerów. Pomimo że powstał pod koniec lat 60. (1969), nadal jest jednym z częściej spotykanych w świecie systemów operacyjnych. Na bazie UNIX-a powstał też „Linux", czyli system przeznaczony dla komputerów osobistych, choć jest on również z powodzeniem używany w komputerach świadczących różne usługi sieciowe.

[69] Open Source (ang.) znaczy otwarte źródło. Terminem tym określane jest oprogramowanie z udostępnionym kodem źródłowym, upoważniającym do swobodnego rozpowszechniania, nieograniczonego używania i dystrybucji, z kodem źródłowym włącznie.

[70] Word Wide Web, zbiór dokumentów odnoszących się do siebie nawzajem dzięki tzw. odnośnikom

[71] HTML (HyperText Markup Language) to język formatowania dokumentów elektronicznych, który pozwala umieszczać tekst oraz połączyć go z grafiką. Dzięki HTML dokumenty mogą łączyć hiper - tekstowe powiązania ("linki") tworząc strukturę, po której porusza się użytkownik Internetu. Obecnie w dokumentach HTML można zawierać dźwięk, animację, sekwencje video, wymaga to najczęściej dodatkowych rozszerzeń, wykraczających poza sam język.

żyjącego na marginesie społecznej aktywności). Hakerów przeraża proces prowadzący niechybnie do uprzedmiotowienia ich twórczej działalności, do wiernego wykonywania poleceń i rozkazów „tyrana", które bez reszty opanują i pochłoną wolność oraz oryginalność. Takie działania władzy uniemożliwiają postęp i rozwój własnego społeczeństwa tkwiącego w karbach reprodukcji. Z tych pobudek i gotowości obrony swoich przekonań hakerzy instynktownie czerpią wrogość wobec cenzury, utajnienia, a także stosowania siły, podstępu czy oszustwa. W założeniu każdy z nich otrzymał mandat na podjęcie wszelkimi dostępnymi sposobami walki z przejawami autorytaryzmu.

Postawa hakerów nie jest jednak wyrazem anarchizmu czy cyberanarchizmu. Taka konkluzja wynika nie tylko z definicji anarchizmu[72], lecz przede wszystkim wypływa z ich założeń, w których widoczny jest brak postulatów obalenia organizacji państwowej, władzy politycznej, ekonomicznej oraz ideologicznej. Hakerzy nie kwestionują konieczności istnienia i funkcjonowania władzy w państwie. Bez niej nawet ich zasady są skazane na niepowodzenie.

Obecność kompetentnych organów państwowych, wykonujących swoje czynności w ramach otrzymanych prerogatyw, jest zjawiskiem ze wszech miar pożądanym przez hakerów – wyznawców kompetencji wspartej na wiedzy i precyzji. Porządek i ład w kraju, walka z kryminalizacją społeczeństwa, prewencja i resocjalizacja, czy pewne przejawy reglamentacji dób i usług są wręcz nieodzownym składnikiem ich koncepcji na „funkcjonowanie" świata. Nazywanie hakera cyberpunkiem, cyberanarchistą, cyberterrorystą jest głębokim nieporozumieniem. Natomiast tzw. "Podziemie" (hakers underground), z pasją opisywane przez publicystów wskazanym jest traktować jako zbiór mający niewiele wspólnego z macierzą, jeśli w ogóle można obie kwestie rozważać na równoległej płaszczyźnie.

Opisując zasady hakerów nie sposób pominąć ich etyki. To bardzo frapujący problem, interpretowany na tyle sposobów, ilu jest hakerów na świecie. Podstawowe zadania etyki – informowanie i pouczanie, jest i w tym wypadku spełnione[73], hhoć górnolotnym poglądem byłoby przyrównanie etyki hakerskiej do jej stricte naukowej postaci (np. normatywnej i metaetyki)[74]. Katalog ich zasad etycznych przypomina bardziej „poradnik", zbiór reguł, który winien być przestrzegany, przynajmniej skłaniać do refleksji. Pomimo, że pierwszy zbiór etyki hakerskiej stworzył S. Levy[75] już w połowie lat osiemdziesiątych ubiegłego stulecia, to nie został do dziś dnia wykreowany jeden obszerny i kompleksowy katalog postępowań. Każdy haker dołącza do niego swoje własne reguły, które uzasadniają, uzupełniają, precyzują i prezentują jego

[72] Por. R. Tokarczyk, Współczesne doktryny polityczne, Kraków 2000, s. 265 – 292; R. Scruton, Słownik myśli politycznej, Poznań 2002, s. 18 – 19; (Red.): M. Chmej , W. Sokół, Mała encyklopedia wiedzy politycznej, Toruń 2001, s. 20; J. Justynski, Historia doktryn polityczno – prawnych, Toruń 2000, s. 353 – 362.
[73] Por. J. Stanisławek, Podstawy etyki, Warszawa 2001, s. 10.
[74] Pisze o tym: R. B. Brandt, Etyka. Zagadnienia etyki normatywnej i metaetyki, Warszawa 1996, s. 14 i nast.
[75] S. Levy, Hackers: Heroes (…), first edition 1984, cyt. za Dr – K, Podręcznik hakera, op.cit., s.10.

postawę. Hakerska etyka jest exemplum wyjaśniającym ich zasady, a czasami ilustrującym postęp cywilizacyjny z całym dobrodziejstwem nowych przestrzeni cyfrowej eksploatacji.

Od etyki hakerskiej należy odróżnić „kodeks Internetu", czyli zasad etykiety sieciowej, tzw. „netykiety" (słowo jest tłumaczeniem angielskiego neologizmu, powstałego z połączenia słów: z ang. net - sieć oraz z fran. etiquette - etykieta). Jest ona zbiorem zasad, norm i dobrych praktyk określających zalecane zachowanie i dobre zwyczaje, których przestrzeganie ułatwia życie wszystkim Internautom[76]. Zasady netykiety w dużej mierze wynikają z praktyki, w domniemaniu dotycząc każdego posługującego się komputerem w sieci. Zasoby globalnej pajęczyny skrywają wiele miejsc zawierających próby kodyfikacji internetowego bon – tonu.[77]. Wiele z sieciowych subkultur – uczestnicy grup dyskusyjnych, IRC, ICQ – wprowadzają własne, specyficzne modele postępowania (netykieta rozpięta jest pomiędzy normami moralnymi a obyczajowymi, twierdzi W. Bober, etyk i autor pracy doktorskiej zatytułowanej „Etyka komputerowa w świetle współczesnej filozofii moralnej")[78]. W gąszczu sieciowego savoir – vivre'u najwięcej zapisów poświęconych jest używaniu poczty elektronicznej, zajmującej, z uwagi na jej tradycję i doniosłość komunikacji interpersonalnych, najwyższą rangę.

Wskazana etyka hakerska i netykieta realizują z wielkim powodzeniem założenia tzw. „samoregulacji" cyberprzestrzeni, będącej alternatywą wobec prawnej regulacji państwowej. Zasady (normy) powstałe w wyniku samoregulacji, to *„(...) prawne reguły, dobrowolnie stworzone przez grupę osób (ewentualnie ich reprezentantów) zaangażowanych w określonego rodzaju działalność, dostępne dla zainteresowanych w stopniu pozwalającym na ich poznanie oraz obwarowane sankcją w wypadku ich nieprzestrzegania (...)"*[79].

Nieodzowną przy próbie analizy fenomenu hakerstwa jest świadomość dokonań i dorobku tych ludzi w dziedzinach informatycznych. Hakerzy mają swój nieoceniony wkład w zbudowaniu sieci Internet, aplikacji sieciowych, czy implementacji sprzętowych. Systematycznie rozwijają system operacyjny UNIX, podejmują żmudną eksplorację systemów i programów komputerowych, testują zabezpieczenia, wyszukują słabe punkty oprogramowania, niejednokrotnie przyczyniając się do jego utylitarnych modyfikacji. Hakerzy stanowią elitę informatyczną, będąc

[76] R. Chmura, Kodeks Internetu, [w:] R. Skubisz (red.), Internet 2000, prawo, op. cit., s. 460.
[77] Por. strony o następujących adresach:
http://kni.ae.krakow.pl/html/netykieta/net_00.html (Jarosław Lech, luty 2000);
http://info.wsisiz.edu.pl/~rrynkiew/netykieta.html (Rafał Rynkiewicz,13.05.2003);
http://forum.gazeta.pl/forum/1,47474,1617503.html; http://www.krokus.com.pl/html/internet/netykieta.html;
http://banita.pl/reg/netykieta.html.
[78] J. Borowski, E – Dżentelmen, „Wprost", nr 912 z 21 maja 2000.
[79] Por. K. Dobrzeniecki, Prawo a etos, op. cit., s. 91 i nast.; W opinii wielu osób efektywnym środkiem eliminacji treści naruszających prawa z internetu pozostają działania samych dostawców usług internetowych (ISP), poprzez samoregulację sieci. Komisja Europejska wspiera również projekt uniwersytecki zajmujący się zagadnieniami samoregulacji. Szerzej na ten temat: http://www.selfregulation.info

tym samym prekursorami postępu cywilizacyjnego. Do ich grona należą wybitni matematycy, inżynierowie, programiści, których żywiołem jest wiedza i informatyka[80].

Hakerzy doceniają rolę informacji, jej niezmierzoną siłę w dobie społeczeństwa informacyjnego. Dostrzegają w niej rękojmię wolności i swobodnego rozwoju ludzkiej cywilizacji. Każdy przejaw reglamentacji, cenzury czy manipulacji informacją (oczywiście w zakresie ich możliwości) jest ustawicznie zwalczany. Nieco dalej posunięte rozumowanie tej postawy zakłada, że wszelkie instytucje prawne regulujące prawo własności, które ogranicza informację (jej dostęp i przepływ), jest zbędne. Zasadą jest wzajemna komunikacja, wolność słowa, wymiana poglądów i wiadomości.

Dążenia hakerów do dogłębnego poznania działania komputerów i sieci nie zawsze bywają zgodne z polityką państw albo globalnych korporacji. W tych kwestiach hakerzy reprezentują nieprzejednane stanowisko: dostęp do Internetu, komputerów i programów powinien mieć każdy bez ograniczeń. Już poprzez swoją obecność wywierają presję na „informatyczne i finansowe giganty", z korzyścią dla odbiorców. W innych sytuacjach proponują alternatywne rozwiązania. Jako przykład można wskazać powszechnie dostępne i pozbawione opłat oprogramowanie z otwartym kodem źródłowym, upoważniającym do jego swobodnego rozpowszechniania, nieograniczonego używania i dystrybucji (zgodnie z założeniami Powszechnej Licencji Publicznej i duchem projektu GNU)[81].

Zdarza się też, że hakerzy świadomie naruszają, a czasami łamią normy prawne. W takich wypadkach należy prześledzić źródło takich czynów, aby dotrzeć do przyczyn determinujących podjęte działania. Stanowią one asumpt do udzielenia odpowiedzi, czy określony czyn wypełniający znamiona przestępstwa został dokonany w celach osiągnięcia korzyści majątkowej, był zwykłym błędem, czy z kolei zamierzonym i kalkulowanym elementem przedsięwzięcia realizującego ważne w ocenie hakerów zadania. Obiektem nadrzędnym jest pogłębienie wiedzy o komputerach, oprogramowaniu, sieciach, a co się z tym wiąże — zwiększanie swoich umiejętności. Dla prawdziwego hakera sam proces "włamywania" jest dużo bardziej satysfakcjonujący niż zdobyte konta czy pliki odkryte w zabezpieczonych, odległych systemach[82].

[80] Charles Babbage, matematyk angielski żyjący w XIX jest uważany za pierwszego hakera, bowiem zaprojektował i skonstruował pracujące urządzenie, uważane za prototyp obecnych maszyn liczących. Szerzej na ten temat: O. Bowcott, S. Hamilton, Hackerzy, op. cit., s. 14 i nast.; W Polsce również istnieje środowisko hakerów, słynące z kompetencji i umiejętności. Do tego grona należy m.in. grupa LSD (Last Stage of Delirium), której rozgłos zapewniło złamanie „niepokonanego Oprogramowania" Argus PitBull (System odparł 5, 25 mln. ataków przeprowadzonych przez 200 tyś. osób. Polskim hakerom wystarczyła zaledwie doba).Szerzej na ten temat: http://lsd-pl.net/.

[81] Szerzej na ten temat: S. Williams, W obronie wolności. Krucjata na rzecz wolnego oprogramowania, Gliwice 2003.; http://www.gnu.org/copyleft/copyleft.pl.html http://www.gnu.org/home.pl.html

[82] D. Doroziński, Hakerzy, op. cit., s. 20.

Przytoczone działania są podejmowane w wyjątkowych okolicznościach, będąc marginalną formą aktywności środowiska. Przy takich założeniach włamania do strzeżonych systemów nie są uznawane za etycznie naganne - przynajmniej do momentu, gdy nie prowadzą do zniszczeń. Poza tym do częstych należą przypadki, gdy po przełamaniu zabezpieczeń systemu haker zgłasza dostrzeżone w nim usterki jego administratorowi, który dzięki temu może zapobiec ewentualnym atakom w przyszłości. Nie jest intencją przypisywać altruistycznych cech każdemu hakerowi oraz usprawiedliwiać czynów, które są przestępstwami, wykroczeniami lub w inny sposób naruszają porządek prawny. Tym niemniej zachowania hakerów, podyktowane interesem jednostkowym, często służą interesom wszystkim podłączonym do Internetu.

W tym kontekście warto zauważyć, że ruch (zjawisko), któremu można nadać miano „rewolucji hakerów" nie jest wyłącznie naukową i teoretyczną himerą. Co więcej, jest nieuniknionym efektem aktywności tych ludzi. Można dywagować o dwóch rodzajach rewolucji: hakerów i quasi hakerów[83]. Subtelną różnicą są założenia obu grup, a co za tym następuje, formy realizacji i wdrażania swoich przekonań. Stąd wniosek, że „rewolucja hakerów" trwa i czasami wzmaga swoje oddziaływanie. Nie jest klasycznym „przewrotem", czy ruchem społeczno – politycznym w tradycyjnym wyobrażeniu, ale procesem, zjawiskiem o nadal nieokiełznanym potencjale.

Hakerzy nie stworzyli doktryny politycznej, nie mają swoich przywódców (ewentualnie duchowych mentorów - zasłużoną starszyznę), nie starają się narzucić swojej ideologii, czy przejąć władzę. Siła, z jaką emanują i kształtują współczesne pojmowanie środowiska hakerskiego, jest traktowana jako czynnik zgoła uboczny. Hakerzy nie aspirują do miana technokratów, nie zabiegają o sławę czy kult, nie pozostają w formalnym zrzeszeniu. Zaledwie kilka reguł, według których postanowili dobrowolnie postępować „hartuje" ich postawę i ducha. Hierarchia wewnątrz grona wynika z zasług i nabytej wiedzy, nie zaś z chęci budowania szkieletu hakerskiej organizacji. Nie jest ich zamiarem stosować przemoc i siłowe rozwiązania, nie dążą do przebudowy sytemu społecznego, politycznego czy ekonomicznego. Występują bardziej w roli romantycznych bohaterów rewolucji postindustrialnej, niż instytucji. Nie muszą walczyć o „przetrwanie", ponieważ postęp technologiczny i rozwój globalnej sieci jest aksjomatem współczesnego świata, zapewniając tym samym stabilizację dla hakerskiej kultury. Prawdziwym zagrożeniem jest erozja ich elitarności i postawy, która nieoczekiwanie doprowadziła do powstania grupy quasi – hakerów.

Współczesny model społeczeństwa jest wyraźnie nakreślony. To zbiorowości bazujące na gromadzeniu, przetwarzaniu i przekazywaniu danych. Wraz z rozwojem społecznej formacji, wyłoniła się grupa ludzi o nadzwyczajnych umiejętnościach i zdolnościach do asymilowania

[83] Na potrzeby publikacji postanowiłem stworzyć dwa terminy: Rewolucji hakerów i quasi hakerów.

cywilizacyjnych przemian. Hakerzy dostrzegają wagę, rolę i doniosłość informacji. Nie bez powodu reguły budujące zręby ich filozofii, wyznaczające idealną postawę hakera, eksponują informację jako immanentny składnik wszelkiego poznania, czyli ich życiowego celu. Dzięki ciekawości, niezłomności i determinacji w rozwiązywaniu problemów uzyskali ogromną przewagę nad pozostałymi członkami społeczeństwa opartego na wiedzy. Mają zawsze o kilka „bitów" więcej informacji niż inni[84]. Dlatego stanowią awangardę społeczeństwa informacyjnego, pełniąc rolę „katalizatora" postępu. Obecność hakerów oraz ich kreatywność wywarła nadzwyczajny wpływ na całą informatyczną infrastrukturę, gospodarkę i współczesną kulturę. Choć rewolucja hakerów jest zjawiskiem mało widocznym i nie do końca poznanym, to z całą pewnością jest fenomenem, który istnieje i promieniuje, głęboko przenikając wszelkie struktury ludzkiej organizacji. Jedynie w domyśle przybiera wymiar techniczny, gdyż w praktyce - etyczny i prospołeczny. Ruch zapoczątkowany przez hakerskie środowisko dopiero rozkwita. Technologia informatyczna stała się tak wszechstronna i tania, że zaczęła już istnieć w naszym życiu niemal niezauważona (jest obecna w artykułach użytku domowego, w bankach i sklepach, w samochodach i samolotach, w szkołach i szpitalach)[85]. Hakerzy w takim otoczeniu mimowolnie stali się grupą ludzi uprzywilejowanych.

Zdumiewające w rewolucji hakerów jest jej podobieństwo do tytułowej „Rewolucji Menadżerów" J. Burnham'a[86]. Zgodnie z koncepcjami autora, menadżerowie to klasa ludzi o kierowniczych aspiracjach i umiejętnościach oraz o niejednolitych poglądach. Co więcej, menadżerowie nie walczą bezpośrednio o swoje cele, nie stworzyli zwartej koncepcyjnie doktryny czy organizacji. Władzę na świecie mieliby zdobyć poprzez systematyczne i konsekwentne przejmowane kontroli nad środkami produkcji, nie tyle w wyniku zmiany tytułów własności, ile w wyniku decydowania przez nią o tym, jak te środki zostaną wykorzystane[87]. Menadżerowie, czyli zespół wszystkich ludzi kontrolujących własność (dyrektorzy, inżynierowie, konstruktorzy) z czasem doprowadziliby do upadku kapitalizmu, ostatecznie przebudowując wszelkie relacje społeczne wraz z ich konotacjami gospodarczymi i politycznymi. Obalenie prywatnej własności, jak i wyrugowanie komunizmu, poprzez stworzenie jednego ogromnego organizmu

[84] A. Fadia, Etyczny hacking, op. cit., s. 17.
[85] Piszą o tym: T. W. Bynum, etyka a rewolucja informatyczna, [w:] (pod red:) A Kocikowski, K. Górniak – Kocikowska, T. Bynum, Wprowadzenie do etyki informatycznej, Poznań 2001, Akademicka Biblioteka Internetowa (adres internetowy: http://abi.amu.edu.pl/aktualnosci.php - wprowadzenie do etyki informatycznej).
[86] Por. J. Burnham, The Managerial Revolution, Penguin Books, London 1962.
[87] Por. H. Olszewski, M. Zmierczak, Historia doktryn politycznych i prawnych, Poznań 1994, s. 359 i nast.

(pewnej globalnej korporacji zarządzanej przez menadżerów) jest konsekwencją oraz ostatecznym etapem rewolucji, która miałaby ogarnąć swym zasięgiem wiele kontynentów [88].

Według Burnham'a menadżerowie – funkcjonariusze bez kapitału, których zasadniczym motywem jest praca i sukces – wraz z nasileniem się roli technokracji zdobywają kontrolę nie tylko nad środkami produkcji, ale także nad państwem, które staje się niejako własnością menadżerów[89]. Proces ten w odczuciu autora jest nieunikniony i skorelowany z elementami konwergencji naukowo – technicznej, która funkcjonuje w podobny sposób we wszystkich krajach, niezależnie od ich ustroju[90]. Rozwój technologiczny pozwalający na stosowanie technik prowadzących do mistyfikacji pobudek i celów podejmowanych decyzji politycznych inspiruje do zdobywania władzy, której mechanizmy sprawowania są takie same w ustrojach socjalistycznych i kapitalistycznych[91]. Z tego tytułu nowa klasa zarządzająca majątkiem przynoszącym znaczne profity z czasem swe zainteresowania skieruje ku władzy politycznej, osiągając swój cel w wyniku rewolucji.

Wprawdzie reżim menadżerów nie rozwinął się na świecie zgodnie z przewidywaniami J. Burnham'a, lecz pokłosie jego koncepcji znalazło wyraz w wielu publikacjach. Ponadto „klasa" menadżerów wpływa istotnie na mechanizmy globalnej gospodarki, a nawet polityki[92]. Słuszne było upatrywanie zalążka rewolucji menadżerów w procesach konwergencji naukowo – technicznej. Równie niebagatelną jest uwaga o identyczności dokonywanych przemian na naszym globie – nie można już dziś ujmować pewnych przemian stosując „lokalny" punkt odniesienia.

Podobnie jak „rewolucja menadżerów" była owocem dokonanych przez autora obserwacji zachodzących zmian - „rewolucja hakerów" jest także wynikiem analiz, badań i bliższego poznania środowiska. W przeciwieństwie jednak do menadżerów, hakerzy nie wyrażają dyrektorskich i dyktatorskich aspiracji. Kluczem ich działalności jest niczym nie skrępowana wolność poznawania i rozwiązywania „fascynujących" problemów. Z racji zainteresowań, koncentrują swoje wysiłki w tym względzie na płaszczyźnie informatycznej. Nie wyrażają wprost przekonań politycznych, nie podejmują dywagacji ekonomicznych, wreszcie nie przewidują oraz nie przejawiają „obsesji" władzy. Kwestie należące go kategorii prawno – politycznych są jakoby pominięte w ich

[88] Pisze o tym: James Burnham and the Menagerial Revolition - Essay on James Burnham, who inspired Orwell when he imagined the geopolitical structure of 1984, form New English *Weekly,* (May 1946), dostępny na stronie internetowej o nastepującym adresie: http://www.k-1.com/Orwell/index.cgi/work/essays/burnham.html.
[89] J. Justyński, Historia doktryn polityczno – prawnych, Toruń 1997, s. 470 – 471.
[90] Ibidem, s. 471.
[91] M. Jaskólski (red.), Słownik historii doktryn politycznych, Warszawa 1997. Tom 1, s. 303.
[92] Obecnie szeroko dyskutowany problem „lobbingu" w Polsce i na świecie. Abstrahując od szczególnej roli przestępstw menedżerskich jakie pełnią w obszarze przestępczości ekonomicznej. Szerzej na ten temat: D. Czajka, Przestępstwa menedżerskie, Warszawa 2000.

koncepcjach. Nie projektują perspektywicznych planów swojej działalności, nie zrzeszają się w hakerski monolit. Stanowią „nieformalną grupę" wyznającą podobne wartości i zasady. Choć i one bywają czasami modyfikowane.

Poza tym nie należy utożsamiać hakingu z haktywizmem będącym jego cybernetyczną odmianą. Przedstawiciele tego ruchu stosują podobne lub identyczne metody działania oraz korzystają z tych samych technologii albo narzędzi co hakerzy. Celem haktywizmu jest protest, który w obecnych czasach, aby został zauważony przez opinię publiczną, przybiera formę cyfrowego alarmu. Haktywiści podejmują żywotne problemy polityczne, społeczne czy ekologiczne w odniesieniu do całego naszego globu. Najczęściej przejawem ich aktywności są włamania do systemów komputerowych lub ataki na strony internetowe instytucji odpowiedzialnych za negatywny – w ocenie haktywistów – stan rzeczy zasługujący na masową dezaprobatę. Oczywiście ruch ten może niebawem przybrać na znaczeniu i oddziaływaniu[93].

De facto spoiwem całej hakerskiej kultury jest podziw i fascynacja technologiami informatycznymi. Ona stanowi najcenniejszy i najważniejszy ich kapitał – wiedzę. Dzięki niej stali się obecni i szczególni. Nawet manifesty hakerów nie są emanacją ich żądań, choć intuicyjnie i terminologicznie rodzą skojarzenia i oczekiwania[94]. W swym zamyśle są raczej wyrazem buntu przeciw ograniczeniom, zwłaszcza natury intelektualnej.

Hakerzy nie tolerują braku kompetencji, odtwórczości, konwencjonalności, ciężkiej i monotonnej pracy, która wpływa uwstecznijąco na istotę ludzką. Hakerzy to błyskotliwi, inteligentni i uzdolnieni ludzie, którzy zawsze zdołają przetrwać i funkcjonować bez względu na panujące konwenanse społeczne. Nie znaczy to, iż dążą do ich obalenia, zmiany czy rekonstrukcji – przeciwnie – zachowują dystans i obojętność. Postawa hakerska jest przecież świadomym wyborem ludzi wolnych.

[93] Por. C. Barker, GIAC Security Essentials Ceretification, SANS Institute 2003, The Hactivism, s. 5 (http://www.sans.org/rr/papers/47/914.pdf).
[94] Por. przykładowy manifest hakera: http://www.geocities.com/tsca.geo/haker.html.