Od propagandy do trollingu – teoria spiskowa czy preludium wojny hybrydowej?

dr Piotr Łuczuk
UKSW

Poza bezpośrednimi cyberatakami na struktury informatyczne, serwery, a nawet serwisy informacyjne to właśnie propaganda w Internecie jest głównym filarem nowej doktryny wojennej – doktryny wojny hybrydowej. Choć o internetowych trollach i propagandzie mówiono już od dłuższego czasu, prawdziwy przełom w tej sprawie miał miejsce zaledwie kilka lat temu.

Na przestrzeni ostatnich lat mogliśmy obserwować wiele przypadków dowodzących jednoznacznie, że przeniesienie działań wojennych do cyberprzestrzeni nie jest już fikcją. Metody prowadzenia wojny hybrydowej opierają się w dużej mierze na działalności wywiadu i kontrwywiadu. Od możliwości zniszczenia infrastruktury informacyjnej przeciwnika ważniejsza jest możliwość pozyskania danych i wyeliminowania dzięki nim systemów bezpieczeństwa.

W działalności wywiadowczej najważniejsze jest pozyskanie informacji. Niezależnie od ich treści mogą się one okazać przydatne w najmniej oczekiwanym momencie. Dlatego w czasie zimnej wojny szpiedzy z narażeniem życia poznawali rytm dnia swoich „obiektów” i gromadzili na ich temat wszelkie możliwe do zdobycia informacje. Teraz rozgrywki szpiegowskie przeniosły się do sieci, gdzie po części to sami użytkownicy napędzają ich działania.

Dla zdolnego hakera przechwycenie danych, haseł czy numerów kont bankowych nie stanowi praktycznie żadnego problemu, ponieważ wielu użytkowników w ogóle nie podejmuje nawet podstawowych środków bezpieczeństwa w pracy z komputerem. Szczególny nacisk na tego typu zagrożenia kładzie również Komisja Europejska, opisując europejskie podejście do umiejętności korzystania z mediów w środowisku cyfrowym (2007).

Scenariusz manipulacji

Etap 1 – rekonesans

Zakłada gromadzenie informacji na temat planowanej akcji oraz analizę docelowych odbiorców. W ramach tych działań zbierane są informacje o osobach potencjalnie zainteresowanych tematem działań, ich lojalności, a także wiedzy w danym obszarze.

Etap 2 – zbrojenia

Zakłada przygotowanie, spreparowanie kluczowej historii i własnej wersji faktów, które następnie mają zostać przekazane docelowym odbiorcom. Ten etap zakłada również przygotowanie dodatkowych fake newsów wspomagających kluczową historię oraz opracowanie różnych „alternatywnych wersji" danego wydarzenia. Prowadzi to do wytworzenia szumu informacyjnego wokół danego tematu i dosłownego zalania Internetu zmanipulowanym przekazem.

Etap 3 – dostawa

Zakłada rozpowszechnianie przygotowanych wcześniej, spreparowanych materiałów i fake newsów za pośrednictwem określonych kanałów komunikacji, np. media społecznościowe lub tradycyjne media. Ponadto działania na tym szczeblu zakładają również możliwość wykorzystania wszelkich możliwych kanałów rozpowszechniania fake newsów, w tym przede wszystkim manipulacji i dezinformacji, za pomocą sieci botów oraz farm internetowych trolli.

Etap 4 – eksploatacja

Zakłada stałe podgrzewanie tematu w mediach społecznościowych i wzmacnianie wiarygodności fake newsów poprzez podsycanie nastrojów konkretnych grup społecznych i sympatyków oraz aktywistów utożsamiających się już z lansowaną ideą.

Etap 5 – utrwalanie

Jeden z kluczowych kroków mających zwiększyć wiarygodność całej akcji propagandowej. Zakłada dotarcie do jak największej grupy docelowej, w tym także do osób nastawionych krytycznie. Głównym celem na tym etapie jest niejako wymuszenie na użytkownikach interakcji i tzw. efektu wirusowego. Im więcej osób będzie pisało/mówiło na dany temat, tym więcej osób o nim przeczyta i usłyszy i w ten sposób wydatnie wzrośnie liczba potencjalnych zwolenników lansowanej idei lub grono osób, które po prostu uwierzą w propagowane w ten sposób fake newsy. Często wykorzystuje się tu wrażenie kłótni na dany temat i preparuje się wpisy o wydźwięku pozytywnym i negatywnym w celu podniesienia rangi fake newsa oraz zwrócenia uwagi osób początkowo krytycznie nastawionych.

Etap 6 – podtrzymanie zaangażowania

Zakłada wprowadzenie do gry przygotowanych na wcześniejszych etapach „historii wspierających” i podsycanie aktywności na możliwie najwyższym poziomie.

Etap 7 – przejście od słów do czynów

Zakłada realizację działań zapowiadanych na początku akcji. Może skutkować dodatkową motywacją docelowego odbiorcy i doprowadzić na przykład do realizacji założonych przez inicjatorów akcji działań, np. organizacji wiecu, manifestacji, apelu poparcia, napisania listu otwartego.

Etap 8 – zacieranie śladów

Zakłada możliwie najszybsze odwrócenie uwagi opinii publicznej od danego problemu i przeniesienie jej, odpowiednie skanalizowanie na zupełnie inny temat. W skrajnych przypadkach etap ten wiąże się nawet z całkowitą negacją i zatarciem pamięci o wszelkich poprzednich działaniach w celu uspokojenia nastrojów społecznych. Takie działanie zapewnia pełną kontrolę nad sytuacją i daje możliwość sprawnego „przełączania" uwagi opinii publicznej na inne tory, z zastrzeżeniem możliwości ponownej aktywizacji grupy docelowej, gdyby w przyszłości zaszła taka potrzeba.

Trzeba poznać jej zasady,

by móc się bronić!

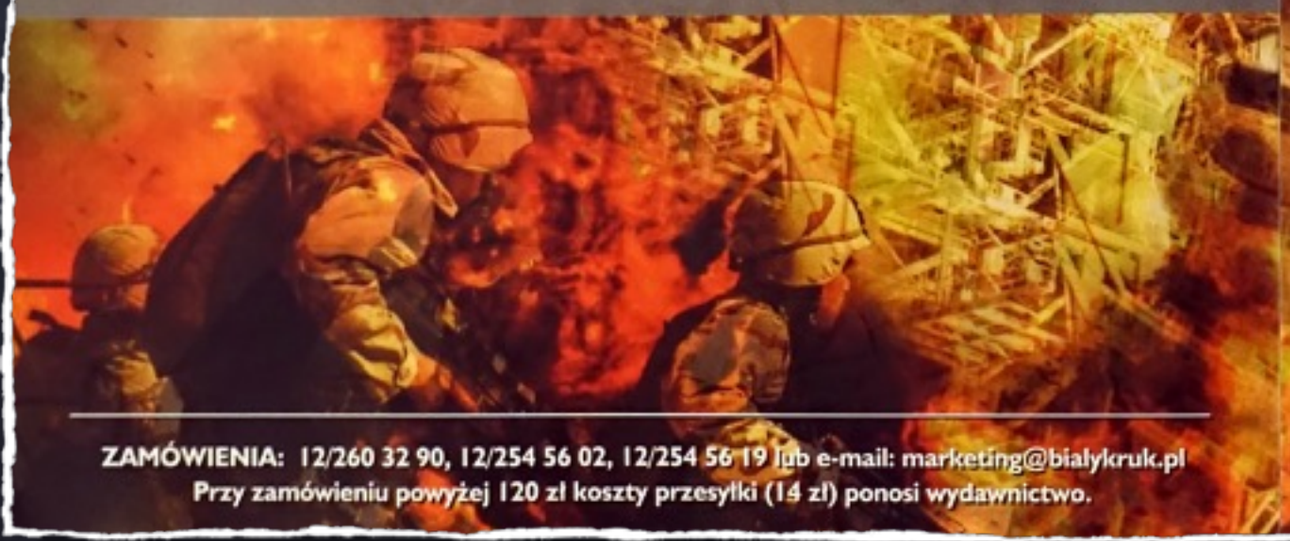
PREMIERA 12.10.2017

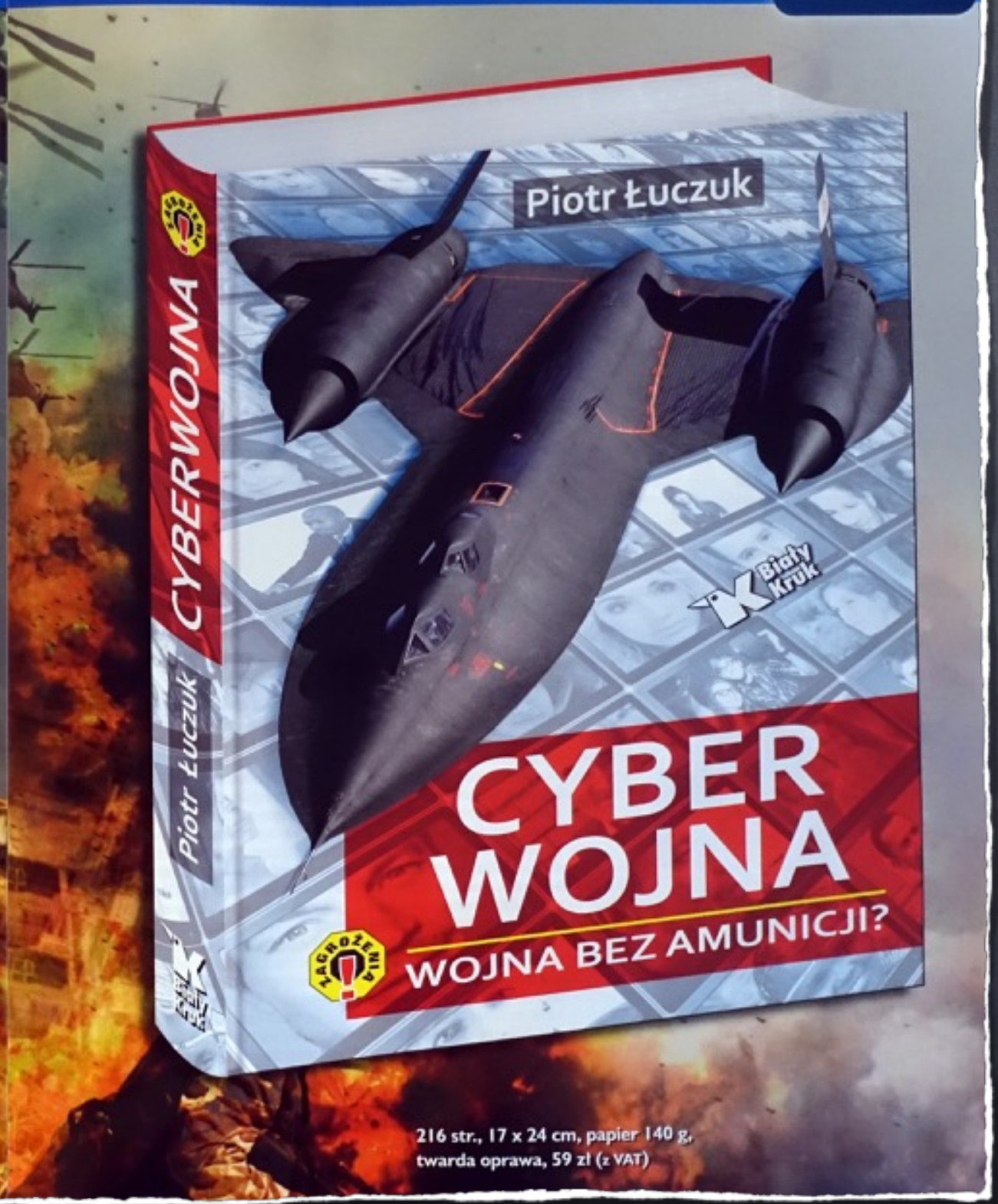
To pierwsza na naszym rynku taka książka rodzimego autora. Opisane w niej wydarzenia, analizy i prognozy nie są bynajmniej dziełem fikcji literackiej. Nie są wyssaną z palca czarną wizją przyszłości. Są niestety jak najbardziej realne. Konflikty wojenne w cyberprzestrzeni, wykorzystywanie potencjału tkwiącego w komputerach, inwigilacja każdego z nas przez globalne sieci – jeszcze do niedawna znaleźć to można było jedynie na kartach powieści *science fiction*. Obecnie nikt nie ma już wątpliwości, że zagrożenia te przeniknęły całkowicie do świata rzeczywistego. Wojny w cyberprzestrzeni stały się dziś jak najbardziej realne. One po prostu już trwają!

Zdolny programista w dowolnym miejscu na świecie, mając do dyspozycji jedynie podłączony do internetu komputer, jest w stanie doprowadzić choćby do wyłączenia prądu w całym regionie, unieszkodliwienia systemów obrony przeciwlotniczej, a nawet do całkowitego paraliżu sektora bankowego. Autor książki dr Piotr Łuczuk podaje bardzo wiele przykładów takich działań hakerów z różnych państw. Hakerów, którzy już nie działają na własną rękę, lecz są ukrytymi żołnierzami.

Choć dzieje się to na naszych oczach, nie dostrzegamy zagrożeń. Bardzo często osoby korzystające z internetu nie są świadome, że same padają ofiarą zmasowanych i doskonale kamuflowanych ataków propagandowych. Żeby ugodzić dziś z wielką precyzją człowieka, równie dotkliwie jak bronią konwencjonalną, wystarczy atak internetowy przy pomocy oszczerstw, pomówień i kłamstw. W powszechnej bowiem opinii to, co napisane i to, co pokazuje obrazek uznawane jest za prawdę. Tymczasem sposobów manipulowania słowem i obrazem, sposobów nękania bliźniego, całych firm, a nawet państw, jest bez liku.

Żeby mieć świadomość, w jakim świecie żyjemy, trzeba koniecznie przeczytać tę książkę. Nie jest to *science fiction*. Ale tak się czyta! Pasjonująca lektura.





ZAMÓWIENIA: 12/260 32 90, 12/254 56 02, 12/254 56 19 lub e-mail: marketing@bialykruk.pl
Przy zamówieniu powyżej 120 zł koszty przesyłki (14 zł) ponosi wydawnictwo.

216 str., 17 x 24 cm, papier 140 g,
twarda oprawa, 59 zł (z VAT)