4

Zwalczanie cyberprzestępczości

Szybki rozwój technologii informacyjnych, coraz większy zasięg internetu oraz gwałtowny wzrost szybkości wymiany informacji sprawia, że ściganie przestępstw w cyberprzestrzeni stało się wyjątkowo trudne. Pomimo trwającej ponad 30 lat debaty na temat cyberprzestępstw wykorzystywanie zdobyczy technologicznych do łamania prawa nadal powoduje poważne problemy zarówno dla ustawodawców, jak i instytucji egzekwujących prawo.

Traktując zwalczanie cyberprzestępczości w kategoriach walki informacyjnej, należy zadbać o wcześniejszą i bieżącą wiedzę o przedmiotach tej walki i otoczeniu. Pozwoli to na dobór trafnych narzędzi i form walki. Walka informacyjna jako działanie celowe jest realizowana w aspekcie osiągnięcia konkretnych zamiarów, tym samym będzie składała się z szeregu równoległych, a także następujących po sobie ogniw rozpoznania i reakcji[360].

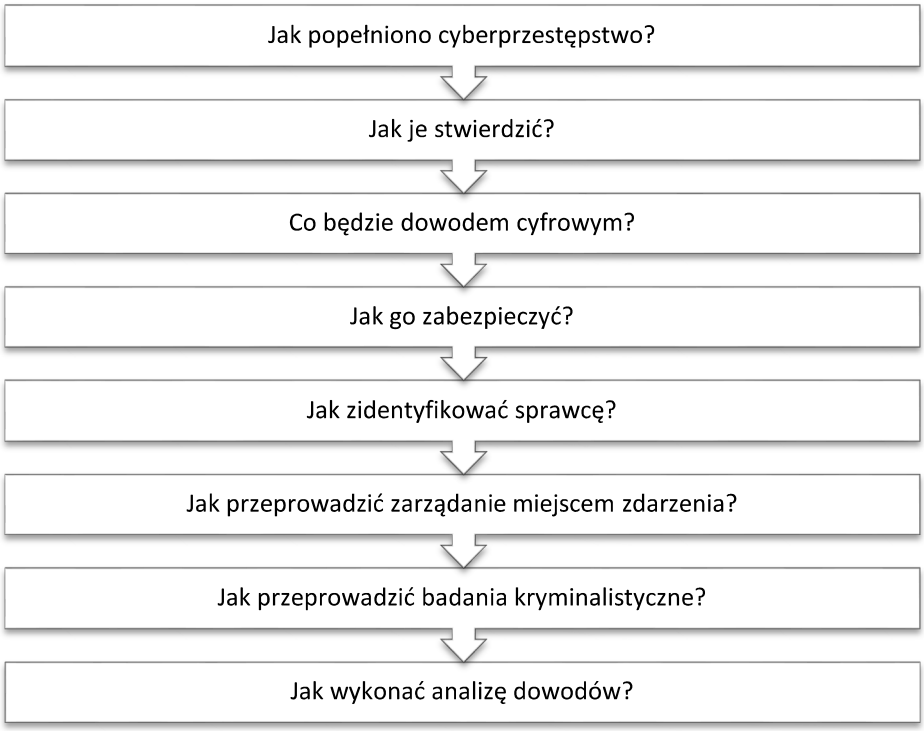
4.1. Model systemu zwalczania cyberprzestępczości

Zwalczanie cyberprzestępczości jest zadaniem skomplikowanym. Wymaga doskonałego zrozumienia nie tylko motywów przestępców i modus operandi przestępstwa, ale – co jest ogromnym obciążeniem – wykorzystanych przez przestępców technologii. Śledczy muszą zrozumieć, w jaki sposób popełniono przestępstwo, i znaleźć potwierdzenie, że miało ono znamiona czynu zabronionego. Poruszając się w świecie śladów cyfrowych, muszą wytypować, odnaleźć, zabezpieczyć, przebadać i w końcu zinterpretować dowody cyfrowe. Biorąc pod uwagę ilość i specyfikę śladów cyfrowych, ich wrażliwość na możliwość manipulacji – świadomej lub nieświadomej, ich zmienność w czasie, muszą je prawidłowo

[360] Por. L. Ciborowski, *Walka informacyjna*, Toruń 2001, s. 89–90.

zabezpieczyć. W wielu przypadkach będzie to tylko część sukcesu, gdyż do wykrycia sprawcy niezbędne jest powiązanie wykrytych urządzeń użytych do popełnienia przestępstwa z konkretnym człowiekiem.

Rysunek 93. Problemy w zwalczaniu cyberprzestępczości

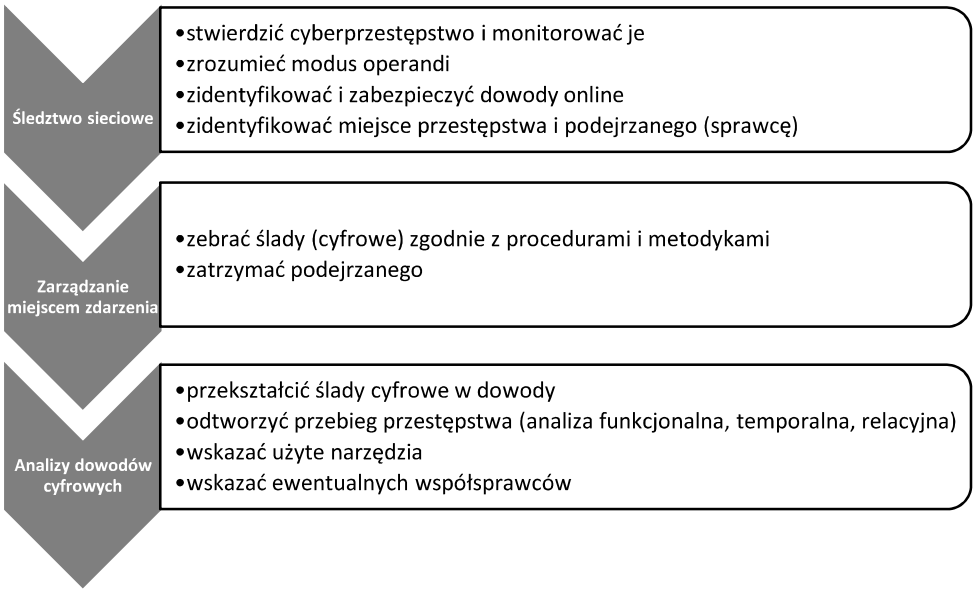


Źródło: opracowanie własne.

Proponowany model systemu zwalczania cyberprzestępczości oparty jest na trzech fazach prowadzenia postępowania. W pierwszej fazie realizowane jest śledztwo sieciowe. Ma ono na celu stwierdzenie popełnienia cyberprzestępstwa, a następnie monitorowanie go, zrozumienie modus operandi, zidentyfikowanie i zabezpieczenie dowodów, które dostępne są online, i w ostateczności zidentyfikowanie miejsca przestępstwa i podejrzanego (sprawcy). W drugiej fazie realizowane są zadania na miejscu zdarzenia. Określenie precyzyjnego miejsca zdarzenia jest bardzo trudne i zwykle nie kończy się na jednym miejscu fizycznym. Na miejscu zdarzenia trzeba zebrać ślady (cyfrowe) zgodnie z procedurami i metodykami oraz jeżeli istnieje taka możliwość, to zatrzymać podejrzanego. W ostatniej fazie prowadzący postępowanie musi przekształcić znalezione i zabezpieczo-

ne ślady w dowody, odtworzyć przebieg przestępstwa (wykonując analizy funkcjonalne, temporalne, relacyjne), wskazać użyte do popełnienia przestępstwa narzędzia i ewentualnych współsprawców.

Rysunek 94. Model systemu zwalczania cyberprzestępczości



Źródło: opracowanie własne.

Praktyczna realizacja przedstawionego modelu przez prowadzącego postępowanie jest możliwa tylko w najprostszych zdarzeniach. W sprawach bardziej skomplikowanych, a takie dominują w cyberprzestępczości, wymagane jest wsparcie i praca zespołowa. Sugerowana struktura jednostki zwalczającej cyberprzestępczość została pokazana na rys. 95.

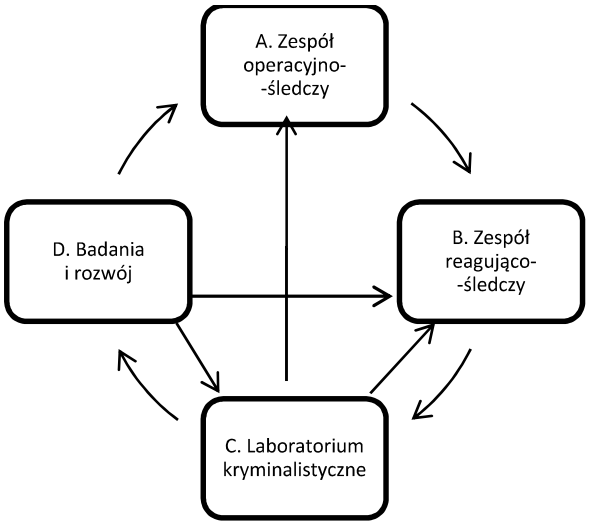
Do zadań poszczególnych proponowanych zespołów należy:

A. Zespół operacyjno-śledczy:
   - prowadzenie aktywnego monitoringu sieci[361],
   - prowadzenie białego wywiadu,
   - prowadzenie działań operacyjno-rozpoznawczych.

[361] Przykładem takiego zespołu może być Centralne Biuro ds. kontrolnych sprawdzeń w zasobach danych (ZaRD) wchodzące w skład wydziału KI26 niemieckiego BKA i zajmujące się „patrolowaniem" Internetu. Zadania realizowane i niedopuszczalne dla funkcjonariuszy ZaRD opisano w: J. Kosiński, C*yberprzestępczość – przegląd wybranych szkoleń*, „Przegląd Policyjny" nr 3/2004, s. 153–166.

B. Zespół reagująco-śledczy:
   – wyszukiwanie urządzeń, w których można ujawnić ślady i dowody cyberprzestępstwa,
   – wykonywanie *triage* i *live forensic* (to zadanie przeszło z laboratorium kryminalistycznego w tradycyjnym modelu do tego zespołu),
   – zabezpieczanie śladów,
   – typowanie podejrzanych.
C. Laboratorium kryminalistyczne:
   – badanie zabezpieczonych śladów, analizowanie danych i informacji, które będą mogły być użyte jako dowody,
   – weryfikowanie hipotez kryminalistycznych.
D. Badania i rozwój:
   – opracowywanie modeli popełniania cyberprzestępczości, opisywanie modus operandi,
   – opracowywanie procedur, przewodników, poradników, dobrych praktyk,
   – przeprowadzanie szkoleń (np. na temat techniki pozyskiwania informacji, wyszukiwania i gromadzenia, nowych technologii, np. cyber lockery),
   – zarządzanie i rozdzielanie informacją (np. dla przemysłu i nauki),
   – opracowywanie narzędzi wymaganych do pracy (np. do monitoringu i przeszukiwania sieci społecznościowych, badania sprzętu telekomunikacyjnego, sprzętu SSD).

Rysunek 95. Proponowana struktura jednostki zwalczającej cyberprzestępczość



Źródło: opracowanie własne.