Bezpieczeństwo 6G

Sieci 6G muszą zapewnić hiperpołączone społeczeństwo, umożliwiające IoE (Internet wszystkiego) służenie swoim celom. Na podstawie tego oświadczenia każdy może wyobrazić sobie, jak ważne jest bezpieczeństwo dla całego ekosystemu 6G, użytkowników, urządzeń i przyszłych usług. Zabezpieczenie złożonej sieci z ultramasywnymi połączeniami i bezproblemową mobilnością będzie wymagało uwagi podczas planowania. W konsekwencji taka złożoność sieci będzie wiązała się z holistycznym podejściem do bezpieczeństwa opartym na bezpieczeństwie jako usługa. 6G Security musi być zaprojektowane tak, aby oferować kompleksowe zabezpieczenia w architekturze sieci 6G i uwzględniać zewnętrznych agentów, którzy będą wchodzić w interakcje z infrastrukturą sieciową od warstwy fizycznej do warstwy aplikacji, w tym wszystkie potencjalne zagrożenia. W związku z tym 6G musi być bezpieczne przez projekt. Wyzwania związane z zapobieganiem i ochroną sieci, urządzeń i społeczeństwa przed cyberterroryzmem są wysokimi priorytetami dla przyszłej sieci bezprzewodowej. Tak więc społeczność naukowa nie może zawieść w tych zadaniach, aby zabezpieczyć sieć 6G. W przeciwnym razie zaufanie do technologii zostanie naruszone, a wszystkie korzyści z niej wytworzone zostaną wykorzystane w najbliższej przyszłości. Zagrożenie to może generować niepewność i niestabilność oraz prowadzić do cyberwojny, która może mieć katastrofalne skutki dla przyszłych sieci bezprzewodowych

Globalne wyzwania związane z cyberbezpieczeństwem - Era cyberprzestępców

Od czasu trzeciej rewolucji przemysłowej, wraz z Internetem, świat skupia się na wszelkiego rodzaju transakcjach elektronicznych, które mają wpływ na zwykłych obywateli, po instytucje państwowe i prywatne. Jak zauważyło Światowe Forum Ekonomiczne, „ponieważ postęp technologiczny i globalna łączność przyspieszają wykładniczo podczas czwartej rewolucji przemysłowej, bezprecedensowe systemowe zagrożenia bezpieczeństwa i zagrożenia podważają zaufanie i wzrost". Dlatego gwarancja zaufanych kanałów telekomunikacyjnych ma kluczowe znaczenie dla globalnej społeczności, zwłaszcza w rozwijającej się gospodarce mobilnej. Na przykład transakcje elektroniczne nie są nowe i można przedstawić wiele przykładów, takich jak mobilne pieniądze, których telefon komórkowy jest używany do dokonywania transakcji finansowych. Jednak w dzisiejszych czasach cyberprzestępczość staje się coraz bardziej modna. Rodzaje cyberprzestępczości są różne, od socjotechniki po zaawansowane międzynarodowe cyberataki na skalę globalną, dotykające państwa i instytucje prywatne, a ta ostatnia jest znana również jako cyberwojna. Dlatego pierwszym międzynarodowym traktatem mającym na celu zwalczanie przestępstw dokonywanych w Internecie była Konwencja Budapeszteńska, znana oficjalnie jako Konwencja o cyberprzestępczości. Konwencja Budapeszteńska została zorganizowana w 2001 roku przez Radę Europy. Konwencja ta uzgodniła zasady i plany działania dotyczące cyberbezpieczeństwa. Poniżej znajdują się opisy przepisów dotyczących ochrony cybernetycznej na podstawie artykułów opublikowanych w traktacie:

• Artykuł 2 – Nielegalny dostęp

• Artykuł 3 – Nielegalne przechwytywanie

• Artykuł 6 – Niewłaściwe użycie urządzeń

• Artykuł 7 – Fałszerstwo komputerowe

• Artykuł 8 – Oszustwa komputerowe

• Artykuł 9 – Przestępstwa związane z pornografią dziecięcą

• Artykuł 12 – Odpowiedzialność korporacyjna

• Artykuł 17 – Przyspieszone zachowywanie i częściowe ujawnianie ruchu danych

• Artykuł 20 – Zbieranie danych w czasie rzeczywistym o ruchu danych

• Artykuł 21 – Przechwytywanie danych dotyczących treści

Aby przeciwdziałać zaawansowanym zagrożeniom cybernetycznym i podkreślić globalną współpracę między narodami, obywatelami i sektorami publiczno-prywatnymi, również ONZ ustanowiło Biuro ONZ ds. Zwalczania Terroryzmu (UNOCT). UNOCT został utworzony w 2017 r. przez ONZ w celu zapewnienia globalnej koordynacji kontrataku i zapobiegania cyberterroryzmowi na całym świecie. Dlatego jak stwierdził ONZ. „Rośnie zaniepokojenie nadużywaniem technologii informacyjnych i komunikacyjnych (ICT) przez terrorystów, w szczególności Internetu i nowych technologii cyfrowych, w celu popełniania, podżegania, rekrutowania, finansowania lub planowania aktów terrorystycznych. Państwa członkowskie podkreśliły znaczenie współpracy wielu zainteresowanych stron w przeciwdziałaniu temu zagrożeniu, w tym między państwami członkowskimi, organizacjami międzynarodowymi, regionalnymi i subregionalnymi, sektorem prywatnym i społeczeństwem obywatelskim”. W tym celu UNOCT podkreśla pięć głównych obszarów koncentracji na cyberbezpieczeństwie:

• Kinektyczne ataki cybernetyczne na infrastrukturę krytyczną i/lub urządzenia IoT

• Rozprzestrzenianie się treści terrorystycznych w Internecie

• Internetowa komunikacja terrorystyczna

• Cyfrowe finansowanie terroryzmu

Ponadto według Narodowej Agencji Bezpieczeństwa (NSA), Science of Security (SoS), jest to rozwijająca się nauka, która musi być zaangażowana we współpracę ze społecznościami akademickimi, promować solidne standardy naukowe i wspierać postęp SoS. W oparciu o te zasady, NSA wskazała pięć głównych wyzwań SoS, którym należy się zająć:

1. Skalowalność i kompozycyjność - rozwój solidnych systemów bezpieczeństwa.

2. Bezpieczna współpraca zarządzana przez zasady – opracowanie skutecznej metodologii obsługi danych dostosowanych do potrzeb różnych użytkowników w różnych dziedzinach urzędów.

3. Ocena, projektowanie, rozwój i wdrażanie oparte na macierzach bezpieczeństwa - opracowanie metryk i mechanizmów bezpieczeństwa w celu określenia i zapobiegania zagrożeniom.

4. Architektury Odporne - opracowanie środków do projektowania bezpiecznych architektur technologicznych.

5. Zrozumienie i rozliczanie ludzkich zachowań - tworzenie metodologie dla użytkowników i przeciwników, które umożliwiają tworzenie i badanie systemów.

Ponadto większość krajów rozwiniętych od wielu lat dysponuje infrastrukturą do zwalczania cyberataków i strategiami politycznymi mającymi na celu ujednolicenie wysiłków na rzecz walki z cyberwojną na szczeblu regionalnym i międzynarodowym. Na przykład w Wielkiej Brytanii istnieje sekcja wojskowa, wywiadowcza 5 (MI5) i słynna Tajna Służba Wywiadowcza (SIS) lub znana również jako (MI6) z filmów o Jamesie Bondzie. Obie organizacje rządowe mają również specjalne wydziały i mnóstwo inwestycji w departamenty cyberbezpieczeństwa, zwłaszcza w celu zapobiegania cyberterroryzmowi, cyberszpiegostwu i atakom na sieci komputerowe. Światowe Forum Ekonomiczne stworzyło również centrum cyberbezpieczeństwa, aby promować globalne partnerstwo w celu przeciwdziałania pojawiającym się na świecie zagrożeniom bezpieczeństwa cybernetycznego. W

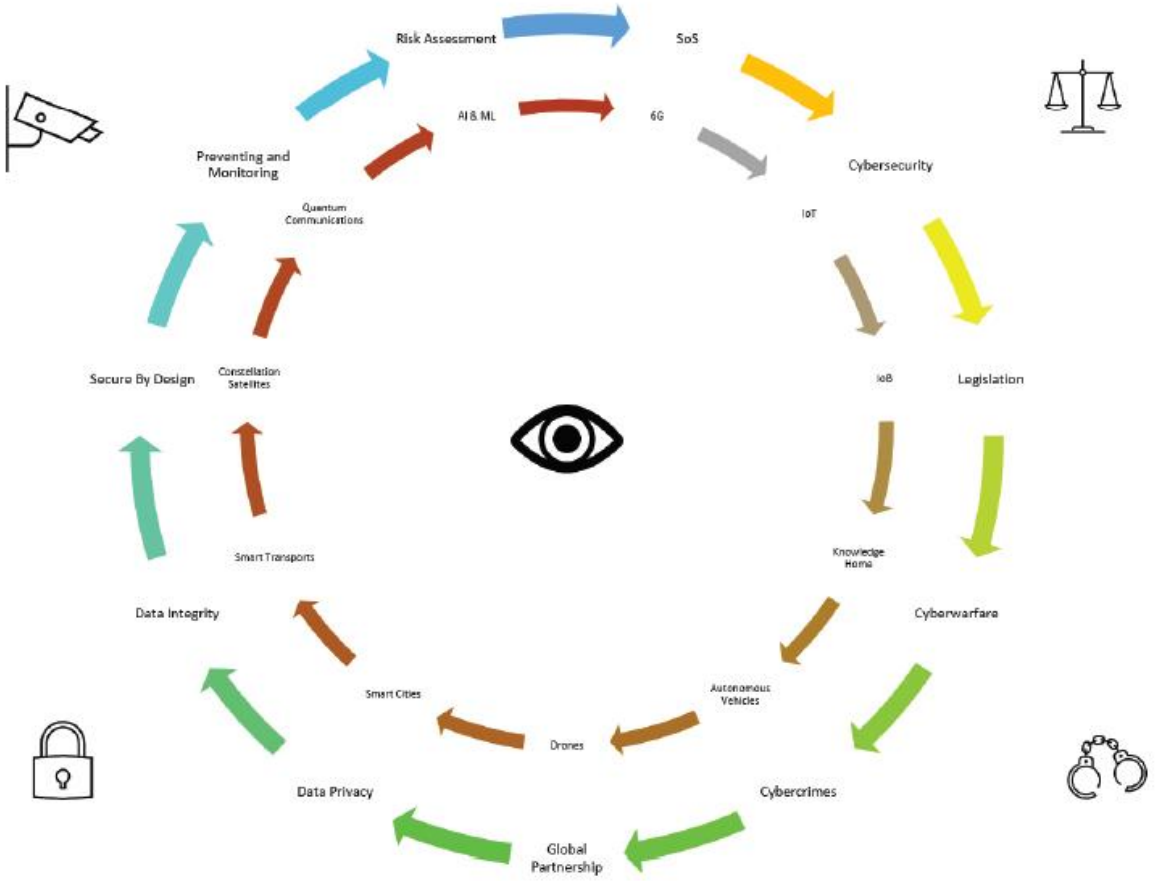
oparciu o tę inicjatywę Światowe Forum Ekonomiczne określiło trzy kluczowe priorytety swojej grupy roboczej:

• Wzmocnienie globalnej współpracy przeciwko cyberprzestępcom

• Zrozumienie przyszłych sieci i technologii

• Budowanie cyberodporności

Rysunek pokazuje na obszarach zewnętrznych cztery filary walki oraz zapobieganie cyberprzestępczości: monitoring cybernetyczny, mechanizmy ochrony cybernetycznej, prawo i wymiar sprawiedliwości oraz wyspecjalizowana policja zwalczająca cyberprzestępczość. Zewnętrzny okrąg pokazuje cyberzagrożenia, działania i polityki. Wewnętrzny krąg przedstawia technologie służące do budowy orkiestracji bezpieczeństwa 6G.



Międzynarodowa Organizacja Policji Kryminalnej (Interpol) utworzyła dział zajmujący się identyfikacją i koordynacją globalnej reakcji na cyberzagrożenia, którego zakres obejmuje:

• Ocena i analiza zagrożeń oraz monitorowanie trendów

• Dostęp i wykorzystanie surowych danych cyfrowych

• Szkolenie cybernetyczne

• Cyfrowa kryminalistyka

• Globalna koordynacja w cyberprzestępczości i dochodzeniach

• Udostępnianie i analiza informacji

• Korelacja informacji cybernetycznych i fizycznych

• E-dowody i procesy zarządzania

• Harmonizacja i interoperacyjność

• Identyfikacja cyberprzestępczości i cyberprzestępców

Według raportu opublikowanego niedawno przez Światowe Forum Ekonomiczne szacuje się, że z powodu cyberprzestępczości światowej gospodarce skradzione zostało około 600 miliardów dolarów. Co więcej, do 2023 r. światowe straty spowodowane cyberatakami mają wynieść 5,2 biliona dolarów. Widać zatem globalne zaniepokojenie rosnącą cyberprzestępczością i cyberterroryzmem na całym świecie. W odpowiedzi na te zagrożenia, wiele światowych organizacji współpracuje, aby zaproponować zaktualizowany system, ustawodawstwo i ramy w celu ochrony danych, osób i sieci przed zagrożeniami cybernetycznymi. W rezultacie orkiestracja cyberbezpieczeństwa 6G ma kluczowe znaczenie dla pomyślnego planu działania dla przyszłych systemów komunikacji bezprzewodowej po 2030 r.

Wraz z ewolucją technologii bezpieczny kanał komunikacji jest wymogiem budowania komunikacji opartej na zaufaniu. Od początku komunikacji bezprzewodowej zapewnienie bezpiecznego kanału RF od końca do końca było problemem dla usług telekomunikacyjnych. Innym ważnym kluczowym czynnikiem bezpieczeństwa jest kodowanie, które przez wiele stuleci było używane przez ludzi do wysyłania zaszyfrowanej wiadomości nieczytelnej dla niezaufanego czytelnika i całkowicie czytelnej dla odbiornika, który musi używać zdekodowanej metodologii. W historii nowożytnej procesy encondingu ewoluowały i były stosowane w usługach telekomunikacyjnych. Na przykład ochrona kanału bezprzewodowego była głównym problemem inżynierów od czasów II wojny światowej za pomocą technik widma rozproszonego, aby uniknąć zagłuszania sygnałów radiowych. Austriacko-amerykańska aktorka Hedy Lamarr (listopad 1904 - styczeń 2000) jako pierwsza zaproponowała technologię widma rozproszonego, która chroniła sygnały radiowe przed zakłóceniami i zakłóceniami. Technika widma rozproszonego zmniejsza zakłócenia sygnału radiowego przesyłającego dane bezprzewodowe na różnych nośnych częstotliwościach. Jednak w latach pięćdziesiątych inżynierowie przeprojektowali tę koncepcję, aby zbudować widmo rozproszenia częstotliwości (FHSS) oparte na algorytmie pseudolosowym do synchronizacji i przesyłania sygnału z różnymi nośnymi częstotliwościami w krótkich odstępach czasu milisekund. Z biegiem czasu technologia bezpieczeństwa sieci ewoluowała, podobnie jak związane z nią zagrożenia. Z tym stwierdzeniem można pomyśleć, dlaczego bezpieczeństwo jest tak ważne? Odpowiedź jest oczywista, ponieważ nie ma zaufania do korzystania z kanału komunikacji bez ochrony, w tym wszelkiego rodzaju usług, od komunikacji głosowej po międzynarodowe transakcje finansowe w czasie zbliżonym do rzeczywistego na światowym rynku akcji. Co więcej, dzięki połączeniu sieci heterogenicznych i wzajemnym połączeniom między enlace RF i sieciami stacjonarnymi, aspekty bezpieczeństwa bezprzewodowego stały się bardziej istotne ze względu na złożoność sieci i potrzebę ochrony wielu aplikacji usług węzłowych. Każda generacja urządzeń mobilnych zawdzięcza część swojego sukcesu orkiestracji bezpieczeństwa zaimplementowanej od dołu warstwy Open Systems Interconnected Model (OSI), która obejmuje warstwę fizyczną (Phy) do góry warstwy aplikacji. Security Service Orchestration (SSO) dla dowolnego kanału komunikacji opiera się na protokołach bezpieczeństwa, kluczach szyfrowania i mechanizmach identyfikacji i potwierdzania powierników sieci, urządzeń zabezpieczających i dodatkowych mechanizmów bezpieczeństwa. W przypadku systemów komunikacji bezprzewodowej nie było inaczej ze względu na kilka stwarzanych im zagrożeń. Zagrożenia te obejmują zarówno odmowę usługi występującą w warstwie PHY, jak i wykorzystywanie luk w zabezpieczeniach aplikacji usługowych. Jak

pokazano powyżej, w mapowaniu tabeli reprezentacja istotnych luk w zabezpieczeniach i zagrożeń jest prezentowana przy użyciu protokołu OSI i protokołu TCP/IP jako odniesienia. Według specjalistów ds. bezpieczeństwa większość słabych punktów bezpieczeństwa w sieciach komórkowych jest związana z protokołami, a nie z fizycznymi częściami sieci. Na przykład protokoły GPRS Tunneling Protocol (GTP) używane w sieciach GSM, UMTS i LTE-A mają lukę w zabezpieczeniach, która może również wpływać na sieci 5G. Powodem tego jest to, że GTP nie weryfikuje geolokalizacji użytkownika, co nie pozwala sieci na poświadczenie, czy ruch przychodzący jest legalny. Słabość tego protokołu może prowadzić do odmowy usługi i oszustwa.

Mapa drogowa bezpieczeństwa 6G

Należy zidentyfikować wszystkie potencjalne zagrożenia, przed którymi stanie przyszła sieć bezprzewodowa. Należy szczegółowo rozważyć architekturę bezpieczeństwa, aby zapewnić pełny wgląd w całą ochronę potrzebną od początkowego uwierzytelnienia urządzenia do zakończenia usługi. Żyjąc w bezprecedensowych czasach wysokiego napięcia między narodami i braku zaufania z powodu globalnych cyberataków i cyberterroryzmu, projektowanie bezpieczeństwa 6G będzie wymagało nowych technologii i metodologii. Najpierw zidentyfikujmy główne obszary 6G i zbudujmy korelację z jej potencjalnymi zagrożeniami. Jak pokazano na powyższym rysunku, przecięcie każdego bloku konstrukcyjnego architektury 6G będzie musiało być ekranowane. Wszystkie potencjalne zagrożenia muszą zostać złagodzone. Na tym polega złożoność robienia tego tylko za pomocą mechanizmów bezpieczeństwa. Jak już wspomniano, w celu zapewnienia bezpieczeństwa należy wdrożyć zaawansowaną orkiestrację sztucznej inteligencji. AI będzie wymagana, głównie ze względu na ogromną liczbę urządzeń podłączonych do sieci oraz konieczność posiadania zaufanego uwierzytelniania i metody ochrony 6G przed wszelkimi cyberatakami. AI zdecyduje, który ruch jest legalny, a który nie. Od pierwszej generacji komunikacji mobilnej bezpieczeństwo jest gorącym tematem ochrony osób i danych. Na początku komunikacji komórkowej najczęstsze zagrożenia bezpieczeństwa dotyczyły intruzów, podsłuchiwaczy, programów typu freeloader, trudnych punktów dostępowych i odmowy usługi (DoS), by wymienić tylko kilka. Jednak czas minął, a zagrożenia bezpieczeństwa stały się jeszcze bardziej wyrafinowane. Skutki naruszenia bezpieczeństwa mogą prowadzić do szkód ekonomicznych, społecznych i psychologicznych. Wszystko zależy od tego, kto lub co jest atakowane w sieci. Z drugiej strony, od danych przemysłowych lub korporacyjnych po poufne informacje osobiste, bezpieczeństwo musi być przedmiotem troski inżynierów, dyrektorów ds. bezpieczeństwa (CSO) i administratorów każdego nowoczesnego systemu. Jest to jeden z powodów, dla których niedawno powstały przepisy dotyczące ochrony danych, takie jak Ogólne rozporządzenie o ochronie danych (RODO) . W tym nowe formy audytorów CISA (Certified Information Systems Auditor) oferujące ustandaryzowane sposoby kontrolowania, nadzorowania i oceny branży teleinformatycznej i telekomunikacyjnej oraz procesów z nią związanych. Wszystkie podatne węzły w sieciach 6G muszą być brane pod uwagę i chronione. Oferuje zaufane protokoły bezpieczeństwa dla otwartych interfejsów API i solidne techniki uwierzytelniania dla połączeń stron trzecich, głównie zlokalizowanych w RAN i MEC, w tym przechowywanie zaszyfrowanych danych. Ponadto rozproszone ataki typu odmowa usługi (DDoS) i ataki podszycia się będą potencjalnym ryzykiem dla ogromnej liczby urządzeń podłączonych do sieci bezprzewodowej, w tym IoT, IIoT i krytycznych usług, takich jak pojazdy autonomiczne, inteligentne domy, a nawet drony. Można sobie wyobrazić, jak katastrofalne może być to, że cyberwojna zostanie uruchomiona na skalę globalną w przyszłym społeczeństwie, które będzie jeszcze bardziej połączone cyfrowo niż obecnie. Stawka za energiczne przyszłe cyberataki w mediach bezprzewodowych jest wysoka, więc łagodzenie ryzyka na wszystkich frontach jest konieczne, aby uniknąć zagrożenia lub zatrzymania życia społecznego. Dlatego stosowana sztuczna inteligencja ze względów bezpieczeństwa oraz systemy obronne, w tym inteligentne firewalle, są niezbędne do stworzenia cyfrowej armii chroniącej 6G. Będzie oferować metodologię bezpieczeństwa ataków

Predict-2-Prevent. Ponadto wymagana jest technologia Distributed Ledger Technology (DLT), która jest później prezentowana jako część 6G Security Orchestration.

Model bezpieczeństwa Blockchain dla 6G

Dlaczego Blockchain jest kwalifikującą się technologią do oferowania metod uwierzytelniania dla 6G? Technologie Blockchain, znane również jako DLT, mają możliwość bezpiecznego przesyłania danych przez Internet za pomocą nieskończonych notatek rejestrujących każdą zmianę, która nastąpiła na danych w sposób zdecentralizowany w czasie rzeczywistym dla wszystkich konsumentów tych danych. Model oferowany przez DLT pozwoli nam zbudować zaufaną sieć bezprzewodową, która jednocześnie jest zdecentralizowana, a wymiana danych nie może być temperowana. Niektóre potencjalne przypadki użycia Blockchain w sieciach 6G to:

• Oferować inteligentne zarządzanie zasobami

• Zapewnienie kontroli dostępu dla 6G i jej zaufanych użytkowników z integralnością danych

• Zapewnij solidną dostępność usług sieciowych, ponieważ Blockchain jest odporny na ataki DDoS.

Jednak same technologie blockchain nie wystarczą. To jest niezbędne do przeanalizowania możliwości zaoferowania firmie Quantum Communications dodatkowej warstwy bezpieczeństwa w kanale komunikacyjnym w infrastrukturze sieci prywatnej i publicznej.

Infrastruktura obliczeń kwantowych dla strategii bezpieczeństwa 6G

Obliczenia kwantowe (QC) nie są nową propozycją technologiczną. Nowością jest przekształcenie obliczeń kwantowych w rzeczywistość ze względu na ich fizyczną złożoność i wyzwania związane z zaprojektowaniem komputera kwantowego, który naprawdę może przestrzegać zasad mechaniki kwantowej. Ojcami założycielami informatyki kwantowej są laureaci nagrody Nobla w dziedzinie fizyki w 1965 r., północnoamerykańscy naukowcy Richard P. Feynman (1918-1988), Julian Schwinger (1918-1994) i japoński naukowiec Sin-Itiro Tomonaga (1906-1979).) za swoje prace w elektrodynamice kwantowej (QED) [90]. QED to pole teorii kwantowej 70 6G Security, które opisuje zachowanie naładowanych cząstek za pomocą pól elektromagnetycznych. Znaczenie tej teorii polega na matematycznym opisie wszystkich oddziaływań zachodzących między światłem a materią i cząsteczkami. Pierwszym, który zaproponował kwantową metodologię obliczeniową opartą na mechanice kwantowej, był północnoamerykański naukowiec Paul A. Benioff. Paul wykazał teoretyczną możliwość wdrożenia komputerów kwantowych w czerwcu 1979 r. Jednak dopiero w 1995 r. matematyk Peter Shor stworzył pierwszy algorytm kwantowy do przetwarzania kubitów [93]. Algorytm ten został ochrzczony algorytmami Shora, a jego wkłady umożliwiły znacznie szybsze rozłożenie na czynniki niż jakiekolwiek klasyczne obliczanie dowolnej liczby całkowitej N przez jej liczby pierwsze. Algorytmy Shora zawierają kwantową transformację Fouriera w swoim algorytmie, a także zdolność do przezwyciężenia słabości szumu kwantowego, która może prowadzić do utraty informacji podczas procesu obliczeń kwantowych. Dzięki algorytmom Shorâ˘A ´ Zs, jeśli teoretycznie istniały, doskonały komputer kwantowy z 4099 kubitami mógłby złamać 2048-bitowy algorytm kryptograficzny Rivesta-Shamira-Adlemana (RSA) w 10 sekund, podczas gdy klasyczny komputer zajęłby około 300 bilionów lat wykonać to samo zadanie. RSA jest jednym z powszechnie stosowanych i bezpiecznych publiczno-prywatnych kluczy szyfrujących w systemach telekomunikacyjnych. RSA jest używany w przeglądarkach internetowych, wirtualnych sieciach prywatnych, w których jeden klucz jest publiczny, a drugi prywatny [95]. Jednak taki komputer kwantowy jeszcze nie istnieje, ale komputery kwantowe stają się rzeczywistością, a IBM

a Google oba mają najwyższy stan wiedzy w dziedzinie obliczeń kwantowych. Podsumowując, obliczenia kwantowe to gałąź mechaniki kwantowej. Różnica między klasycznymi obliczeniami dotyczy reprezentacyjnych stanów zer lub jedynek. W obliczeniach klasycznych podstawową jednostką jest bit, który ma tylko jeden stan logiczny, czyli zero (0) lub jeden (1). Może być również reprezentowany na dwóch poziomach napięcia, które mogą być na przykład napięciem O lub napięciem +1, jako reprezentacja fizyczna. W informatyce kwantowej istnieje kubit, który jest kwantowym stanem reprezentacyjnym, w którym wynik może wynosić od 0 do 1 lub dowolną wartość pomiędzy. Ta zdolność cząstek kwantowych do jednoczesnego uzyskiwania obu wyników nazywana jest superpozycją. Dopiero gdy nastąpi interferencja kwantowa, cząstka kwantowa zapada się i każdy może zobaczyć reprezentacyjny stan cząstki kwantowej. Następnie, po zapadnięciu się, jedynym sposobem na powrót do stanu kwantowego jest zresetowanie cząstki kwantowej. Ale w skrócie, znaczenie obliczeń kwantowych polega na tym, że mogą one przekroczyć całą moc komputera istniejącą w klasycznym systemie obliczeniowym. Wyzwaniem dla komputera kwantowego jest to, że na razie nie istnieje programowalny język obliczeń kwantowych, a naukowcy wciąż opracowują dla niego metodologie, a także nie istnieje standardowa architektura komputera kwantowego, jaka istnieje w przypadku komputerów klasycznych. Wszystkie istniejące komputery kwantowe mogą przetwarzać kubity i wymagają bardzo niskiej temperatury pokojowej do wykonywania zadań opartych na stanach kwantowych. Odkładając na bok wyzwania związane z obliczeniami kwantowymi, ewolucja komputerów kwantowych w ciągu najbliższych dziesięciu lat może doprowadzić do kolejnej rewolucji przemysłowej i pozwoli na sprawne i sprawne wykonywanie złożonych codziennych zadań w erze niezmierzonego tworzenia Big Data po 2030 r. W tej perspektywie komputery kwantowe mogłyby zostać połączone ze sztuczną inteligencją, aby zarządzać ogromną ilością Big Data wymienianą na brzegu i w rdzeniu sieci 6G oraz umożliwiać inteligentne zarządzanie ruchem dla różnych typów aplikacji usługowych, zapewniając jakość doświadczenia. W tym celu przewiduje się obecnie połączenie sił uczenia maszynowego i obliczeń kwantowych. Rezultatem jest nowo proponowana technologia o nazwie Quantum Machine Learning (QML) do szybkiego śledzenia inteligentnego przetwarzania danych i statystycznej analizy wzorców danych. Wdrożenie klasycznego przetwarzania jako szybszej odpowiedzi na przyszłe wyzwania stojące przed 6G byłoby nieskuteczne. Haven powiedział, że ewolucja informatyki kwantowej przyniosłaby również przewidywalne wyzwania, takie jak niebezpieczne cyberzagrożenia w przypadku, gdy komputery kwantowe wpadną w ręce cyberprzestępców lub cyberterrorystów. Aby zwalczyć to przyszłe zagrożenie, analizuje się obecnie pewne strategie kryptograficzne i sieciowe, które mają być wykorzystywane jako środki ochrony przed atakami z wykorzystaniem obliczeń kwantowych. Obecnie badania opierają się na kryptografii Lattice-Based Cryptography i Hash-Based Signatures. Oba są silnymi kandydatami do użycia ze względu na szyfrowanie ochronne i stają się kryptografią odporną na kwanty. Inną odpowiedzią na cyberataki kwantowe byłoby zbudowanie kwantowej sieci komunikacyjnej opartej na szyfrowaniu kwantowym, jak przedstawiono w podrozdziale 6.6.

Komunikacja kwantowa

Aby zabezpieczyć kanał komunikacyjny, wymiana kluczy szyfrujących jest konieczna do zaszyfrowania danych przed wysłaniem i odszyfrowania po przybyciu do miejsca docelowego tylko przez odbiorcę. Jednak wymiana zaszyfrowanych kluczy między nadawcą a odbiorcą wiąże się z wieloma zagrożeniami bezpieczeństwa. Zagrożenia te są jeszcze bardziej widoczne ze względu na sztuczną inteligencję i zaawansowane rodzaje cyberataków. Google przedstawił niedawno raport, z którego wynika, że 94% ruchu jest szyfrowane . Z jednej strony ten trend pokazuje rosnące przekonanie, że szyfrowanie danych dominuje w kontekście prywatności danych, ale niekoniecznie przekłada się to na bezpieczeństwo. Podstawowe technologie szyfrowania są oparte na Secure Socket Layer/Transport Layer Security

(SSL/TLS) i HyperText Transfer Protocol Secure (HTTPS). Jednak w sieci mogą wystąpić luki w zabezpieczeniach, które mogą prowadzić do naruszenia bezpieczeństwa. Niektórzy z nich są:

• Luki w certyfikatach

• Złośliwe oprogramowanie

• Kradzież poświadczeń

• Zaszyfrowana złośliwa witryna

• Szyfrowane oprogramowanie ransomware

Dlatego niezbędne są zaawansowane rozwiązania bezpieczeństwa, aby uniknąć istniejących i przyszłych zagrożeń w sieci. W oparciu o to założenie Komisja Europejska i ESA tworzą ramy do opracowania zaawansowanego systemu szyfrowanej komunikacji skoncentrowanego na komunikacji kwantowej. Przewidywany projekt nosi nazwę misji Security And cryptoGraphic (SAGA). To nie jedyna grupa projektowa i badania skoncentrowane na mechanice kwantowej w celu rozwiązania problemów związanych z bezpieczeństwem. Istnieje wiele innych. Ale projekt Saga daje wgląd w przyszłe możliwości komunikacji kwantowej. Ale czym jest komunikacja kwantowa? Komunikacja kwantowa opiera się na zasadach mechaniki kwantowej, w których „technologie wykorzystują transfer informacji kwantowej z jednego miejsca do drugiego. Technologie te sięgają od wykorzystywania nieodłącznej losowości pomiarów kwantowych do wytwarzania wysokiej jakości kluczy kryptograficznych w celu dzielenia się sekretami (kryptografia kwantowa, pieniądze kwantowe, aukcje kwantowe, głosowanie kwantowe, zaangażowanie kwantowe...) po przesyłanie pełnych informacji kwantowych, np. z jednego procesora kwantowego do drugiego za pomocą teleportacji stanu kwantowego.” Jedną z jego możliwości jest wymiana Kwantowej Dystrybucji Klucza (QKD). W tym procesie nadawca może szyfrować komunikację za pomocą bezpiecznych losowych kluczy, chroniąc kanał komunikacji przed podsłuchem i podsłuchem. Gdy intruz spróbuje przełamać kanał bezpieczeństwa, kanał komunikacji kwantowej unieważni kanał komunikacyjny. Właśnie dlatego infrastruktura komunikacji kwantowej (QCI) jest tak ważna dla przyszłej komunikacji bezprzewodowej. Powstanie więcej usług i aplikacji związanych z obliczeniami kwantowymi i komunikacją kwantową, prowadząc z przedstawionej perspektywy do następnej fazy Internetu kwantowego. Aby uzyskać więcej informacji na temat technologii Quantum, czytelnicy mogą odwiedzić Flagship Quantum Technologies