GRUPO INTER-GOVERNAMENTAL DE ACÇÃO CONTRA O BRANQUEAMENTO DE DINHEIRO EM ÁFRICA OCIDENTAL

RELATÓRIO REGIONAL



TIPOLOGIAS DE BRANQUEAMENTO DE CAPITAIS E FINANCIAMENTO DO TERRORISMO LIGADAS À CIBERCRIMINALIDADE NA ÁFRICA OCIDENTAL

Maio 2025

O Grupo Inter-Governamental de Acção contra o Branqueamento de Dinheiro (GIABA) é uma instituição especializada da CEDEAO e um órgão regional do tipo GAFI que promove políticas para proteger o sistema financeiro dos Estados membros contra o branqueamento de capitais, o financiamento do terrorismo e o financiamento da proliferação de armas de destruição maciça. As Recomendações do GAFI são reconhecidas como a norma mundial de combate ao branqueamento de capitais (LBC) e ao financiamento do terrorismo (CFT).

Para mais informações sobre o GIABA, visite o site: www.giaba.org

Este documento e/ou qualquer mapa aqui incluído não prejudicam o estatuto ou soberania sobre qualquer território, a delimitação de fronteiras e limites internacionais nem o nome de qualquer território, cidade ou área.

Referência:

Relatório de Tipologias do GIABA (2025), o Branqueamento de Capitais e o Financiamento do Terrorismo Ligado a Cibercrimes na África Ocidental, GIABA, Dakar, Senegal

© GIABA 2025. Direitos reservados.

Nenhuma reprodução ou tradução desta publicação pode ser feita sem uma autorização prévia por escrito. Os pedidos de autorização para divulgar, reproduzir ou traduzir a totalidade ou parte desta publicação devem ser dirigidos ao GIABA, Complexe Sicap Point E Av Chiekh A. Diop, X Canal IV 1er Etage Immeuble A, BP 32400, Ponty Dakar (Senegal). Correio eletrónico: secretariat@giaba.org Fax: +221 33 824 17 45

AGRADECIMENTOS

O Diretor-geral gostaria de agradecer o apoio prestado pelos Estados membros do GIABA na realização deste estudo de tipologias. O GIABA está particularmente grato aos seus Correspondentes Nacionais (CNs) e aos pesquisadores dos países pelos seus esforços no processo de recolha de dados, especialmente na mobilização das partes intervenientes nacionais e na facilitação do acesso atempado da equipa de pesquisa junto às agências e instituições relevantes a nível nacional.

O estudo beneficiou do enorme apoio dos serviços responsáveis pela aplicação da lei, dos serviços de informações, do sistema judicial, de outros organismos profissionais e da sociedade civil dos Estados membros. Estas instituições/agências asseguraram que a equipa de pesquisa se reunisse com os principais intervenientes e fornecesse as informações necessárias, em alguns casos a prazo muito curto.

O GIABA também gostaria de reconhecer a colaboração excecional dos nossos parceiros de desenvolvimento, particularmente o GAFI e o OCWAR-C, pelo tempo que dedicarem para fazer a revisão do relatório em várias etapas e, assim, enriquecê-lo. Os membros do Grupo de Risco, Tendências e Métodos (GRTM) e do Grupo de Revisão de Políticas (GRP) do GIABA também trabalharam em colaboração com o Secretariado para melhorar a qualidade global deste relatório.

Também queremos reconhecer os esforços individuais dos membros da equipe do projeto, que trabalharam ininterruptamente para assegurar a coordenação e conclusão adequadas do Projeto, sob a supervisão do Diretor de Políticas e Pesquisas, Sr. Muazu Umaru. O nosso agradecimento especial vai também para o nosso colega Sr. Lansana Daboh (Oficial de Monitorização do Risco), cujo empenho tem sido fundamental na produção e finalização deste relatório. Outros membros da equipa de pesquisa dignos de reconhecimento são a Senhora Mairo Ladidi Abass, a Senhora Ramatoulaye Barry Diop, o Senhor Saer Kamara e o Senhor Idrissa Ouattara.

Secretariado do GIABA

ÍNDICE

AGRADECIMENTOS **3**
SUMÁRIO EXECUTIVO **6**

CAPÍTULO 1 - INTRODUÇÃO **9**
Contexto geral 9
Motivação para o estudo 10
Objetivo 11
Metodologia do estudo 11

CAPÍTULO 2 - A PREVALÊNCIA DA CIBERCRIMINALIDADE NA ÁFRICA OCIDENTAL **13**
A dicotomia entre cibercrime e cibersegurança 13
Prevalência da cibercriminalidade na África ocidental 14

CAPÍTULO 3 - ESTUDOS DE CASO DE TIPOLOGIAS DA CIBERCRIMINALIDADE DE BC E FT NA ÁFRICA OCIDENTAL **16**
Tipologia 1: Fraude com Cartões Eletrónicos (crédito/débito) 16
Tipologia 2: Fraude / Esquemas de violação de Caixas de correio (Email) 17
Tipologia 3: Violação/Fraude informática nos sistemas corporativos (website/base de dados) 20
Tipologia 4: Fraude através do pagamento Adiantado de Taxas e Branqueamento de Capitais 23
Tipologia 5: Fraude através do Esquema Ponzi e Branqueamento de Capitais 36
Tipologia 6: Fraude relacionada com dinheiro móvel e branqueamento de capitais 40
Tipologia 7: Casos de Financiamento do Terrorismo facilitados pela Cibernética 44

CAPÍTULO 4 – SINAIS DE ALERTA E INDICADORES **47**
Indicadores 47
Sinais de alerta 48

CAPÍTULO 5 - QUADRO JURÍDICO, REGULAMENTAR, DE SUPERVISÃO E DE EXECUÇÃO E OS DESAFIOS ASSOCIADOS **50**
Quadro Jurídico, Regulamentar e de Execução para a Cibersegurança / Cibercrime na África Ocidental 50
Instituições responsáveis pela luta contra a cibercriminalidade na África Ocidental 54
Ratificação de instrumentos internacionais 58
Desafios jurídicos, regulamentares e de execução 60

CAPÍTULO 6 – CONCLUSÃO E RECOMENDAÇÕES **62**
Conclusão 62
Recomendações 62
Referências 62

ANEXO A: MODELO DE ANÁLISE DE CASOS **65**

GRUPO INTER-GOVERNAMENTAL DE ACÇÃO CONTRA O BRANQUEAMENTO DE DINHEIRO EM ÁFRICA OCIDENTAL (GIABA) **72**

LISTA DE ABREVIAÇÕES E ACRÓNIMOS

IA:	Inteligência Artificial
BC:	Branqueamento de capitais
LBC:	Luta contra o branqueamento de capitais
FT:	Financiamento do terrorismo
CFT:	Combate ao financiamento do terrorismo
FP:	Financiamento da proliferação
CFP:	Combate ao Financiamento da Proliferação
IoT:	Internet das Coisas - IdC
CENTIF:	Célula Nacional de Tratamento de Informação Financeira
ANR:	Avaliação Nacional do Risco
CUA:	Comissão da União Africana
EFCC:	Comissão de Crimes Económicos e Financeiros da Nigéria
GIABA:	Grupo Inter-Governamental de Acção contra o Branqueamento de Dinheiro em África Ocidental
CEDEAO:	Comunidade Económica dos Estados da África Ocidental
GAC:	Grupo de Avaliação e Conformidade
GRTM:	Grupo de Riscos, Tendências e Métodos
GRP:	Grupo de Revisão de Políticas
RAM:	Relatório de Avaliação Mútua
DNS:	Distribuição de Negação de Serviço
VEC:	Violação de Emails Corporativos
NPF:	Força Policial da Nigéria
EOCO:	Escritório de Crimes Económicos e Organizados
COS:	Comunicações de Operações Suspeitas
VA:	Ativo virtual
VASP:	Prestador de serviços de ativos virtuais
TIC:	Tecnologias de Informação e Comunicação
LTA:	Agência de Telecomunicações da Libéria
CIF/UIF:	Unidade/Centro de Informação Financeiro
UIF-N:	Unidade de Informação Financeira da Nigéria
OCWAR-C:	Crime Organizado: Resposta da África Ocidental sobre Cibersegurança e Cibercrime
GAFI:	Grupo de Ação Financeira
NATCOM:	Comissão Nacional de Telecomunicações
BoG:	Banco do Gana
UE:	União Europeia

SUMÁRIO EXECUTIVO

1. O espaço de ataques digitais expandiu enormemente, passando para o trabalho remoto, de mais pessoas em linha (conectadas) e de maior interconectividade de computadores e dispositivos inteligentes em todo o mundo. Com o desenvolvimento das tecnologias digitais, a utilização das redes de informação e comunicação como instrumento para facilitar os fluxos financeiros ilícitos está a crescer como um dos principais desafios na resolução do problema da circulação de fundos ilegais. As novas ferramentas digitais para transferências de dinheiro, tais como serviços bancários em-linha e móveis, pagamentos eletrónicos, criptomoedas, prestadores de serviços de comércio eletrónico e serviços de jogo em-linha, especialmente se forem combinados, oferecem um número incontável de oportunidades para distanciar o dinheiro das suas fontes ilegais de lucro ou para transferir ilegalmente dinheiro de fontes legais. A pandemia da COVID-19 também criou novas oportunidades para os criminosos fazerem uso abusivo e indevido dos sistemas financeiros através das tecnologias de forma mais inovadora e complexa.

2. Face ao que precede, fica muito claro que as tecnologias digitais representam problemas significativos para o combate ao branqueamento de capitais, ao crime organizado e ao financiamento do terrorismo, uma vez que os ciberataques continuam a evoluir e a aumentar em frequência e nível de sofisticação. Os recentes relatórios do GIABA revelam, de forma flagrante, a prevalência de crimes cibernéticos, tanto como uma importante fonte de produtos do crime quanto como um veículo de fundos criminosos na região. Parece que todos os tipos de crimes associados às tecnologias digitais na região são sistematicamente difíceis de tratar, não só devido às lacunas regulamentares e de aplicação da lei, mas também devido à falta de conhecimentos especializados e infraestruturas adequadas. Na maioria dos países membros do GIABA, a cibercriminalidade constitui uma ameaça séria para as economias nacionais que exige uma resposta coerente e colaborativa a nível regional. É igualmente necessário acordar e harmonizar as normas a nível internacional, a fim de reduzir o risco de lacunas e de arbitragem regulamentar.

3. Consciente deste desafio complexo, o GIABA realizou este estudo de tipologias sobre Branqueamento de Capitais e Financiamento do Terrorismo ligados ao Cibercrime na África Ocidental. Apesar da gravidade deste fenómeno, a cibersegurança ainda é considerada um luxo, e não uma necessidade, em muitas economias africanas. A sua importância ainda não foi suficientemente apreciada nem reconhecida. Tendo em conta o exposto, é imperativo a realização desses exercícios de tipologias, pois, estes irão alimentar as bases de uma fundação estrutural e regulamentar da luta contra a criminalidade informática na África Ocidental.

4. O estudo visa melhorar a compreensão sobre os riscos de branqueamento de capitais ligados ao cibercrime entre os Estados membros do GIABA, apresentar políticas, conformidade e aplicação aprimoradas. As constatações do estudo irão revelar as implicações para as intervenções e, a este respeito, serão apresentadas recomendações relevantes. O relatório pretende lançar luzes sobre as diferenças entre cibersegurança e cibercrimes e a magnitude de ambos os fenómenos na África Ocidental e, ainda, a prevalência do crime. Explorará, também, os fatores de risco de BC/FT associados à cibercriminalidade na região e identificará as técnicas e os métodos mais comuns adotados para o branqueamento dos produtos da cibercriminalidade. Ainda, apontará as vulnerabilidades mais críticas e conducentes a riscos acrescidos de branqueamento dos produtos da cibercriminalidade e apresentará medidas políticas e programas orientados para ação que poderão ser adotados com base nas constatações do estudo.

5. A metodologia adotada foi de uma abordagem multilateral que incluiu o Secretariado do GIABA, grupos de peritos e um perito dos Estados membros. As principais constatações do estudo incluem uma dicotomia entre cibersegurança e cibercriminalidade, a natureza predominante dos casos cibernéticos e os métodos, técnicas e tendências do crime na África Ocidental. O estudo revelou que a África Ocidental tem registado um aumento na conectividade à Internet acima da média da África Subsariana. Esta conectividade é, no entanto, variável e dispersa. A taxa de conectividade na África Ocidental varia entre 70% (Cabo Verde) e 15% (Níger). Os ganhos obtidos em relação ao aumento da conectividade à Internet estão a ser corroídos pelo ritmo exponencial em que a cibercriminalidade está a ser perpetrada e as consequências são terríveis e prejudiciais.

6. Com base em entrevistas realizadas pelos pesquisadores nacionais, existe uma visão convergente de que as autoridades policiais na região parecem sobrecarregadas, uma vez que 2 em cada 3 infrações relatadas estão relacionadas com a cibercriminalidade. Isso ficou mais evidente durante o pico do período da COVID 19 (2020 – 2021). Um diagrama no Capítulo 2 apresenta uma evidência ilustrada da prevalência da cibercriminalidade na África Ocidental e descreve a extensão (estimativa) em que os vários tipos de casos estão a ser perpetrados. O mais prevalente dos casos (40%) enquadra-se no tipo de fraude através do pagamento adiantado de taxas. Segue-se-lhe o tipo de casos relacionados com dinheiro móvel (15%), seguido do tipo de casos do esquema Ponzi (13%). Os outros tipos de casos mais prevalentes são violação de sites ou plataformas comerciais (7%), e casos combinados de DNS (Distribuição de Negação de Serviços) e violação de caixas de correio eletrónico corporativos (7%). Os casos menos relatados são as fraudes com cartões de crédito/débito e os casos relacionados com o financiamento do terrorismo.

7. Dos 52 casos identificados, que parecem descrever o fenômeno, foram abstraídas sete tipologias distintas. As tipologias incluem fraude com cartões eletrónicos (crédito/débito); fraude/golpe de violação de e-mails; violação e fraude dos sistemas corporativos/organizacionais; fraude através de pagamento adiantado; Fraude usando o esquema Ponzi; fraude relacionada com dinheiro móvel; e casos de financiamento do terrorismo facilitados pelo espaço cibernético. Os indicadores e os sinais de alerta confirmam que a informalidade, a falta de sensibilização do público para as ameaças cibernéticas, os recursos inadequados investidos na cibersegurança por parte das empresas e das instituições/organizações públicas, a fraca arquitetura, e os sistemas regulamentares e a monitorização do panorama cibernético na região e os fracos sistemas de aplicação da lei têm um efeito espiral na cibercriminalidade e na criminalidade facilitada pela cibernética no branqueamento de capitais e financiamento do terrorismo na África Ocidental.

8. Existem lacunas legislativas significativas nos países, particularmente em relação aos poderes da autoridade central responsável pela luta contra a cibercriminalidade e aos quadros jurídicos e de repressão/execução dos países para detetarem, provarem e travarem eficazmente o branqueamento de capitais ou o financiamento do terrorismo associados à cibercriminalidade. Embora o quadro jurídico e de repressão/execução preveja medidas de aplicação da lei para investigar e processar os cibercriminosos, o quadro regulamentar na maior parte dos países da África Ocidental tem medidas preventivas insuficientes ou é globalmente fraco. Embora alguns poucos países tenham obtido alguns ganhos nessa área, a obtenção de provas eletrónicas e digitais durante uma investigação continua a ser um desafio em algumas jurisdições.

9. Em linha com as exigências das normas globais, em particular, nos termos da Recomendação 36 do GAFI sobre Cooperação Internacional, que incentivava os países a ratificarem outros instrumentos e convenções internacionais relevantes, como a Convenção de Budapeste e as Convenções de Malabo, a região da África Ocidental tem envidado esforços e realizado progressos consideráveis na luta contra a cibercriminalidade, a par de outros crimes subjacentes. Mas estes esforços e progressos também teem sido acompanhados de desafios, entre os quais, questões como lacunas na legislação, má interpretação por parte das instituições do seu mandato, capacidade técnica limitada, recursos humanos e materiais inadequados e a falta de colaboração e coordenação. Além disso, a cooperação internacional é ainda muito fraca.

10. Embora exista uma vasta gama de métodos e técnicas utilizados pelos cibercriminosos para branquear o produto das suas atividades criminosas, os investigadores e os procuradores realizaram poucas ou nenhumas investigações financeiras paralelas após terem detetado os cibercrimes. Eles também são, em muitos casos, confrontados com a dificuldade de estabelecer provas da infração de cibercriminalidade devido à falta de tecnologia e equipamento necessários, à coordenação nacional integrada ineficaz entre as unidades operacionais em matéria de LBC/CFT e à falta de implementação de mecanismos de cooperação regional e internacional.

11. Para que a luta contra a cibercriminalidade seja mais eficaz e dissuasora, o estudo apresenta recomendações tanto para as autoridades públicas como as autoridades competentes na luta contra a cibercriminalidade. É necessário lançar e intensificar campanhas de sensibilização destinadas ao público, promover uma cultura de cibersegurança na região e apoiar os países no estabelecimento de um quadro jurídico e institucional em conformidade com as normas internacionais atualmente em vigor. É preciso realizar uma avaliação de riscos adequada e criar Laboratórios Forenses Digitais para apoiar as provas forenses para as AALs e reforçar as capacidades operacionais dos investigadores em matéria de técnicas de investigação digital e colmatar a lacuna existente entre o quadro jurídico e a legislação especial LBC/CFT/CFP, a fim de facilitar e acelerar a instauração de processos penais contra os cibercrimes.

12. Criar um Fórum Regional de Plataformas Nacionais de Combate à Cibercriminalidade na África Ocidental para permitir que as autoridades competentes funcionem em redes e partilhem dados e informações. Monitorizar a assinatura, ratificação e incorporação de instrumentos internacionais e desenvolver capacidades em matéria de deteção, investigação, ação penal e julgamento de casos de cibercrime e como seguir o dinheiro, incluindo a realização de investigações paralelas e financeiras.

CAPÍTULO 1

INTRODUÇÃO

Contexto geral

13. As tecnologias emergentes como carros autónomos, Inteligência Artificial (IA), *Machine Learning*, Automação, Virtualização, Cidades Inteligentes, Redes *Blockchain*, *Big Data*, *Internet das Coisas* (IoT), Internet dos Sentidos, Nuvem e Computação Quântica, etc. estão a criar mudanças operacionais que exigirão novos requisitos de segurança cibernética. Nos últimos dois anos, a área de ataque digital expandiu-se muito devido a uma mudança em direção ao trabalho remoto - mais pessoas em-linha e mais interconectividade de computadores e dispositivos inteligentes em todo o mundo.

14. Simultaneamente, as empresas criminosas aproveitaram-se da falta de visibilidade e de administração da segurança. Com o desenvolvimento das tecnologias digitais, a utilização das redes de informação e comunicação está a aumentar enquanto um instrumento para facilitar os fluxos financeiros ilícitos. Este é um dos principais desafios na resolução do problema da circulação de fundos ilegais. Escusado será dizer que as tecnologias digitais facilitam os fluxos financeiros ilícitos em cada fase, seja ganhando dinheiro ilegalmente, transferindo fundos ilegais ou usando esses fundos. Existem vários domínios em que se pode estabelecer ligações claras entre a tecnologia e os fluxos financeiros ilícitos.

15. Além da criação dos mercados ilegais do submundo de cibercrimes e crimes relacionados à cibernética, as tecnologias digitais facilitam a migração do crime organizado tradicional em-linha e oferecem várias oportunidades de fraude, corrupção, evasão fiscal, entre outras atividades criminosas. Novas ferramentas digitais para a transferência de dinheiro, como serviços bancários em-linha e móveis, pagamentos eletrónicos, criptomoedas, comércio eletrónico e jogos de azar em-linha oferecem um número incontável de oportunidades para distanciar o dinheiro das fontes ilegais de lucro ou para transferir ilegalmente dinheiro das fontes legais, especialmente se forem conjugadas.

16. Além disso, as novas formas de negócios em-linha e a economia digital facilitam a transferência de lucros ilegais e a agregação de fundos ilícitos em contas *offshore*, a sua colocação em empresas de comércio eletrónico falsas e em negócios em-linha *offshore*. A pandemia da COVID-19 também criou novas oportunidades para os criminosos abusarem dos sistemas financeiros através das tecnologias de uma forma mais inovadora e complexa.

17. Face ao que precede, fica muito claro que as tecnologias digitais colocam problemas significativos para o combate ao branqueamento de capitais, ao crime organizado e ao financiamento do terrorismo. Os ciberataques continuam a evoluir e a aumentar em frequência e sofisticação. Essa é a razão pela qual a cibercriminalidade se tornou uma importante área de atenção e investimento em todo o mundo.

18. Na África Ocidental, o nexo entre o branqueamento de capitais/financiamento do terrorismo (BC/FT) e a cibercriminalidade é flagrante. Enquanto o BC/FT se tenha desenvolvido devido à globalização financeira (ou seja, a capacidade de todos os agentes económicos e sociais utilizarem os serviços financeiros a nível internacional), a cibercriminalidade está a aumentar devido à globalização tecnológica através do desenvolvimento da Internet e de ferramentas conexas. O relatório do GIABA sobre a implantação de Fintech (tecnologias financeiras), frequentemente manchetes de notícias, relatórios anuais de atividades apresentados pelos Estados membros do GIABA e os seus relatórios sobre as Avaliações Nacionais de Risco (ANR) de BC/FT, os resultados de avaliações mútuas e processos de seguimento, todos revelam de forma flagrante a prevalência de crimes cibernéticos, tanto como uma importante fonte de produtos do crime quanto como um veículo de fundos criminosos na região. Parece que todos os tipos de crimes associados às tecnologias digitais na região são sistematicamente difíceis de tratar, não só devido às lacunas regulamentares e de aplicação da lei, mas também devido à falta de conhecimentos especializados e de infraestruturas adequadas.

19. Na maioria dos países membros da GIABA, a cibercriminalidade constitui uma séria ameaça para as economias nacionais que exige uma resposta coerente e colaborativa a nível regional. As falhas de algumas jurisdições no combate ao cibercrime ameaçam a segurança, a estabilidade e a eficácia dos governos, das infraestruturas críticas, das empresas e dos indivíduos em toda a região. É necessário uma governação resiliente para assegurar que as agências relevantes em todas as jurisdições cooperem entre si (por exemplo, entre supervisores, UIF e outros organismos operacionais em matéria de prevenção da criminalidade ou de aplicação da lei). As normas nacionais também têm de ser acordadas e, possivelmente, harmonizadas a nível regional, se não internacional, a fim de reduzir o risco de lacunas e de arbitragem regulamentar, principalmente para fins transnacionais. Além disso, a falta de consistência e de harmonização entre as jurisdições tem impulsionado os custos de conformidade.

20. Consciente deste desafio complexo, o GIABA realizou este estudo de tipologias sobre Branqueamento de Capitais e Financiamento do Terrorismo ligados ao Cibercrime na África Ocidental.

Motivação para o Estudo

21. A maioria das economias africanas caracteriza-se pela permissividade dos regimes regulamentares, que proporcionam um terreno fértil para as atividades de cibercriminalidade. De acordo com um relatório de novembro de 2016 da Comissão da União Africana (CUA) e da empresa de cibersegurança Symantec, dos 54 países de África, 30 careciam de disposições legais específicas para combater o cibercrime e lidar com provas eletrónicas. As autoridades policiais em alguns países não tomam medidas significativas contra *hackers* que atacam sites internacionais. Por exemplo, foi relatado que algumas autoridades na Nigéria alegaram que não tinham conhecimento de crimes cibernéticos originários no país, enquanto alguns rotularam-no como propaganda ocidental. Alguns altos funcionários eleitos do Estado também estariam envolvidos em crimes cibernéticos. Em 2003, a Comissão de Crimes Económicos e Financeiros da Nigéria (EFCC) deteve um membro da Câmara dos Representantes da Nigéria pelo seu alegado envolvimento em atividades relacionadas com cibercrimes.

22. A classificação dos casos de cibercrime de acordo com o país de origem (CUA, 2016) dos queixosos menciona três países africanos entre os 50 mais afetados: África do Sul em 11.º lugar (434 queixas), Nigéria (24.º lugar, com 215 queixas) e Egito (45.º, com 95 queixas). Quando os casos são classificados de acordo com os danos causados, os queixosos sul-africanos estão novamente na primeira posição, com 6,5 milhões de dólares perdidos, seguidos pela Nigéria (2,9 milhões de dólares) e Egito (523.000 dólares). O surgimento destes crimes ligados a transações por telefone fica mais acessível pelo uso generalizado de métodos de pagamento de dinheiro móvel.

23. Em relação à fraude da caixa de cartões SIM, isso custou à Côte d'Ivoire 926 milhões de francos CFA em 2014. Esta técnica permite que os fraudadores contornem os canais usuais das telecomunicações internacionais, que são então tratados como chamadas locais, resultando na arbitrariedade de tarifas. Esta situação causa enormes prejuízos às empresas de telecomunicações. No Senegal, embora haja poucos dados disponíveis, o caso mais significativo envolve uma empresa de transferência de dinheiro cujo site foi hackeado por várias horas em 2020. Os *hackers*, que diziam ser senegaleses, queriam chamar a atenção para a questão da segurança. A primeira página do site tinha uma página preta com um texto dos dois criminosos. Eles disseram, entre outras coisas, que a segurança cibernética é negligenciada no país e sua ação foi realizada para lembrar os interessados da importância da segurança cibernética.

24. Apesar da gravidade deste fenómeno, a cibersegurança ainda é considerada um luxo e não uma necessidade em muitas economias africanas. A sua importância ainda não foi suficientemente apreciada ou reconhecida. Segundo relatos, os orçamentos destinados à cibersegurança em muitas organizações são inferiores a 1%, e muitas organizações tinham um orçamento zero alocado para a cibersegurança. No entanto, as tecnologias digitais têm potencial para servir de instrumento para combater o problema do branqueamento de capitais e do financiamento do terrorismo. Podem servir como uma fonte de empoderamento e transparência, e podem ser usados em investigações, deteção e interrupção das transferências ilegais de dinheiro.

25. Face ao que precede, impõem-se a realização de um exercício exaustivo de tipologias. Tal exercício alimentará os fundamentos de uma base regulamentar estrutural e sólida para combater a criminalidade informática na África Ocidental e, ainda, atirará mais luzes sobre as ameaças da cibercriminalidade e a medida em que está a exacerbar outros crimes subjacentes ao branqueamento de capitais, incluindo o branqueamento de capitais e o financiamento do terrorismo na região do GIABA.

Objetivo

26. Este estudo de tipologias visa melhorar a compreensão dos riscos de branqueamento de capitais associados ao cibercrime entre os Estados membros do GIABA, visa melhorar a política, a conformidade e a execução/repressão. Os resultados revelarão as implicações para as intervenções e serão apresentadas recomendações relevantes. O relatório pretende abordar as seguintes questões específicas:

a) Qual a diferença entre cibersegurança e cibercrime? E qual é a magnitude dos fenómenos relacionados na África Ocidental?

b) Quais são as diferentes formas de atividades criminosas através de tecnologias digitais nos Estados membros da GIABA?

c) Quais são os fatores de risco do BC/FT associados aos cibercrimes na região?

d) Quais são as técnicas e métodos mais comuns adotados para o branqueamento dos produtos das atividades de cibercrimes na África Ocidental?

e) Quais são as vulnerabilidades (sistémicas) mais críticas que conduzem a riscos acrescidos de branqueamento dos produtos da cibercriminalidade?

f) Quais são as medidas políticas e os programas orientados para a ação que podem ser adotados com base nas constatações do estudo para mitigar eficazmente os riscos de BC/FT associados às tecnologias digitais?

Metodologia do Estudo

27. Como prelúdio da metodologia, o estudo foi concebido durante os vários encontros e discussões nos fóruns técnicos do GIABA e reuniões para discustir os seus vários relatórios (GRTM/GRP e reuniões de peritos do GAC e reuniões plenárias) - os RAMs, relatório de avaliação das Fintech, de Avaliação de Riscos particularmente dos Ativos Virtuais e VASP) entre 2021 e início de 2022. A metodologia detalhada e posteriormente adotada inclui o seguinte:

Uma **sessão de brainstorming de 3 dias** foi organizada em **julho de 2021** para refletir sobre os principais problemas relacionados a esta questão, bem como o escopo do projeto. A sessão contemplou apresentações de representantes dos Estados membros sobre a situação prevalecente em matéria de cibercriminalidade nos respetivos países. Os membros dos grupos GRTM/GPR também contribuíram para o efeito.

Uma sessão virtual de *brainstorming* foi realizada em **setembro de 2021** e o resultado dessas duas (2) sessões ajuda na finalização do conceito do projeto e dos Termos de Referência detalhados para recrutar os membros da equipa do projeto dos Estados membros do GIABA.

Foi constituída uma equipa de projeto, composta por 15 Pesquisadores de País (um perito recrutado em cada Estado membro da CEDEAO), membros dos grupos GRTM e GPR do GIABA e apoiada pelo Secretariado do GIABA em **julho de 2022**).

Recolha e análise de dados (aplicação de questionários, incluindo a realização de entrevistas aprofundadas com uma série de autoridades relevantes, agências de combate à cibercriminalidade, instituições financeiras, bem como vítimas de cibercrimes e outros indivíduos vulneráveis) – (**julho-setembro de 2022**).

Análise dos relatórios dos países apresentados por peritos e análise exaustiva dos padrões, métodos, técnicas e impacto do fenómeno e uma análise crítica das constatações, incluindo o seguimento a nível nacional, conforme necessário – **setembro-outubro de 2022**).

Apreciação dos relatórios dos países no Seminário Regional Anual de Exercícios de Tipologias do GIABA – **outubro 2022**).

Elaboração de um relatório abrangente, incluindo recomendações específicas e gerais que contribuam para a formulação de políticas e intervenções operacionais contra o BC/FT relacionados com a cibercriminalidade, tanto a nível nacional como regional – (**março-abril de 2023**).

Tradução e revisão da qualidade do projeto de relatório consolidado para as 3 línguas da CEDEAO – **abril - maio de 2023**.

Revisão e validação à distância pelos Estados membros, observadores, parceiros de desenvolvimento, membros do GRTM/GRP e outros intervenientes – **maio de 2023**.

Apreciação e aprovação do relatório pelo plenário do GIABA - **maio de 2023**.

CAPÍTULO 2

A PREVALÊNCIA DA CIBERCRIMINALIDADE NA ÁFRICA OCIDENTAL

28. Este capítulo procura analisar e apresentar a dimensão e os tipos de cibercrimes perpetrados na região da África Ocidental, tendo em conta o volume de casos de cibercrimes denunciados diariamente e a (in)capacidade das autoridades policiais de investigar todos os casos. É também de salientar que o número de casos ou ocorrências comunicados às autoridades policiais não se traduz necessariamente em investigações, uma vez que vários casos ou ocorrências denunciados (dezenas e centenas de denuncias) podem estar relacionados e resultar num único caso. O capítulo analisará algumas questões contextuais e de definição antes de discutir os tipos de casos prevalentes na região, conforme relatados.

Dicotomia entre cibercrime e cibersegurança

29. O cibercrime é uma atividade criminosa que envolve um computador, dispositivo de rede ou rede, diretamente direcionado para danificar ou desativar computadores e dispositivos, espalhando *malware*, por exemplo, roubando informações secretas, etc., cometida principalmente para fins lucrativos. Os cibercrimes ocorrem quando um computador/dispositivo de rede/rede for (a) visado, ou (b) ser incidental ao crime, ou (c) utilizado diretamente para perpetrar o crime. Enquanto (a) e (b) são principalmente devido a vulnerabilidades no sistema, (c) é uma ameaça direta ao sistema. Além disso, embora (a) tenha a ver com o nível de alerta, sensibilização e preparação do público em matéria de cibersegurança (todas as pessoas singulares e coletivas), (b) envolve a capacidade política, regulamentar e de aplicação da lei para prevenir e interromper a cibercriminalidade, incluindo a gestão eficaz da arquitetura e ambiente informático jurisdicional (domínio público).

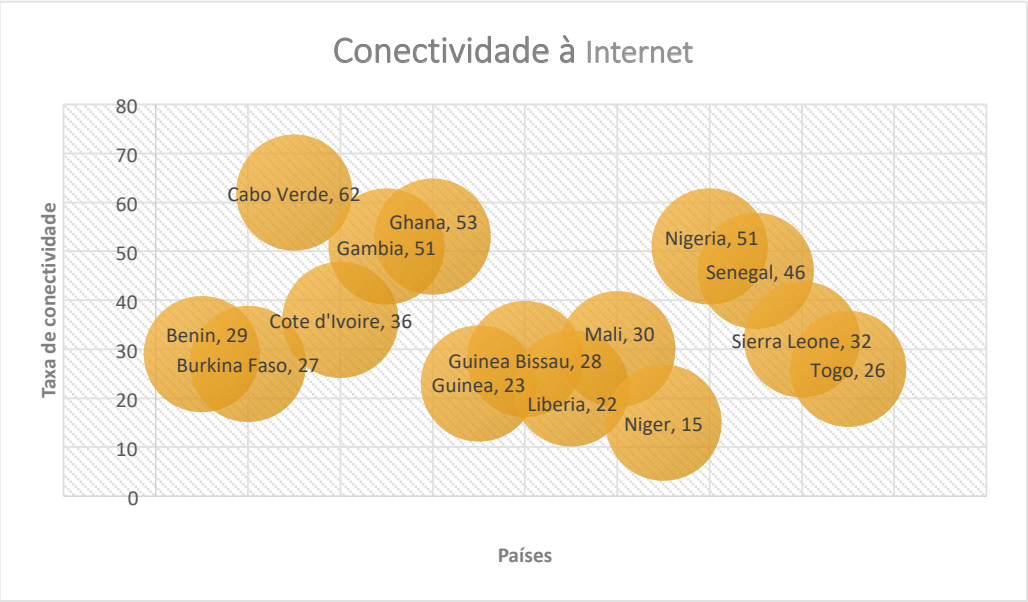
30. Cibersegurança é a tecnologia e o processo concebidos para proteger redes e dispositivos contra ataques, danos ou acesso não autorizado. A cibersegurança visa proteger as organizações, aumentando assim a eficiência e a produtividade, inspirando confiança no cliente/parceiro. Os aspetos da cibersegurança incluem a proteção de dados e a proteção dos sistemas das organizações para prevenir ataques. A cibersegurança é um requisito operacional importante para qualquer agente económico e é exigida principalmente por três (3) razões principais, ou seja, os princípios da confidencialidade (informações e funções a serem acedidas apenas pelas partes autorizadas), integridade (informações e funções a serem adicionadas, alteradas ou removidas apenas pelas partes autorizadas) e disponibilidade da informação (sistemas, funções e dados devem estar disponíveis quando solicitados de acordo com parâmetros acordados com base nos níveis de serviço).

31. A prevenção e interrupção da cibercriminalidade são um efeito importante da cibersegurança. O processo de garantir que um sistema está protegido contra a intrusão e o uso abusivo não se limita apenas a tomar os vários passos para ter múltiplas camadas de autenticações e senhas complexas, *firewalls* e antivírus com criptografia em servidores de nomes de domínio seguros, mas também, realizar atualizações regulares e avaliar riscos (identificar, monitorar e avaliar ameaças) e implementar mitigantes para os riscos identificados. Embora a cibersegurança possa ajudar a prevenir determinados cibercrimes, nem todos os crimes (facilitados pela cibernética) podem ser prevenidos apenas com uma boa segurança.

Prevalência da cibercriminalidade na África Ocidental

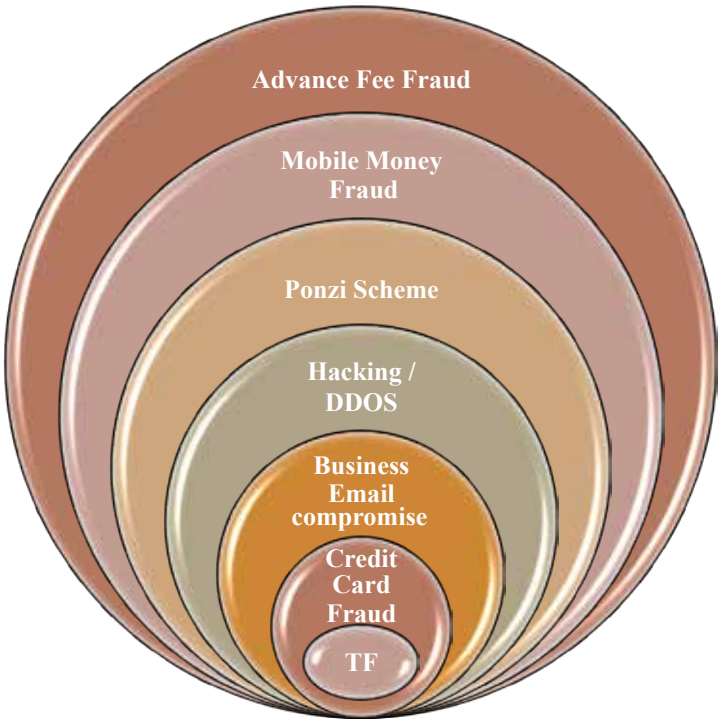
32. Embora o estudo (no capítulo seguinte) apresente os vários tipos de tipologias presentes na África Ocidental, esta seção apresenta a prevalência do crime sem aprofundar nas técnicas e métodos detalhados utilizados para perpetrar o crime. A África Ocidental tem assistido a um aumento da conectividade à Internet acima da média da África Subsariana. Esta conectividade é, no entanto, variável e dispersa. A taxa de conectividade na África Ocidental é de o máximo 70% (Cabo Verde) e tão baixo quanto 15% (Níger). Os ganhos obtidos em relação à conectividade à Internet conduzem a um ritmo exponencial de perpetração da cibercriminalidade. As suas consequências são terríveis e prejudiciais. Abaixo está um diagrama (Figura 2.1) que mostra a taxa de conectividade à Internet na região.

Figura 2.1: A Conectividade Internet na África Ocidental



33. Com base nas entrevistas realizadas pelos pesquisadores nacionais, existe uma visão convergente de que as autoridades policiais na região parecem estar saturados, uma vez que 2 em cada 3 infrações comunicadas estão relacionadas com a cibercriminalidade. Isso ficou mais evidente durante o pico do período da COVID 19 (2020 – 2021). O diagrama que segue apresenta uma evidência ilustrada da prevalência da cibercriminalidade na África Ocidental e descreve a extensão (estimativa) em que os vários tipos de casos estão a ser perpetrados. O mais prevalente dos casos (40%) enquadra-se no tipo de fraude através de pagamentos adiantados. A seguir está o tipo de casos relacionados com dinheiro móvel (15%), seguido do tipo de casos de esquema Ponzi (13%). Em seguida, o tipo de casos mais prevalentes é *hacking* ou violação de sites ou plataformas comerciais (7%) e casos combinados de DNS (Distribuição de Negação de Serviços) e violação de caixas de correio eletrónico corporativos (7%). Os casos menos comunicados são as fraudes com cartões de crédito/débito e os casos relacionados com o financiamento do terrorismo.

Figura 2.2: Prevalência e tipos de crime na África Ocidental



Quadro 2.1: Prevalência e Tipos de Crimes com Média Ponderada na África Ocidental

Tipo de crime	Média ponderada	Descrição específica / título do crime
Fraude através de pagamento adiantado de taxas	0.39	Esquemas usando ouro, extortion sexual, pornografia infantil, extorsão, fraude de romance corporativo com empresas de fachada, fraude de recrutamento de emprego, fraude de proposta de negócio, fraude com contrato de exportação, fraude de serviço de frete, fraude usando esquema de herança, tráfico de seres humanos e sequestro, falsificação e chantagem, fraude e falsificação de identidade
Fraude através de dinheiro móvel	0.15	Falsas pretensas, falsificação de identidade e falsificação, fraude com cartões SIM, abuso de informação privilegiada e pirataria informática, fraude de agentes de dinheiro móvel, roubo de identidade através de cartões SIM pré-ativados a partir de registo de eleitores abandonado
Fraude do esquema Ponzi	0.14	Esquema de negociação on-line, fraude esquema Ponzi, esquema Ponzi ativo virtual, investimento on-line / fraude do mercado de valores mobiliários, investimento em dinheiro móvel esquema Ponzi, fraude de investimento de comércio eletrônico, fraude de empréstimo em linha
Pirataria informática/ DNS	0.12	Pirataria informática em websites, hacking business platform, DNS, Insider dealing / Funcionário comprometido, hacking de conta de mídia social e falsificação de identidade, insider dealing e esquema fraudulento de facilidade de crédito
Violação de emails corporativos	0.10	BEC, *phishing* e fraude usando esquema de violação de e-mails
Fraude com cartão de crédito	0.06	Roubo de cartão de crédito/débito, fraude com cartão de crédito/débito
Relacionado com FT	0.06	FT baseado no comércio, suspeita de angariação de fundos para FT, *hawala* para FT

CAPÍTULO 3

ESTUDOS DE CASO DE TIPOLOGIAS SOBRE CIBERCRIMES DE BRANQUEAMENTO DE CAPITAIS E FINANCIAMENTO DO TERROSIMO NA ÁFRICA OCIDENTAL

34. Este capítulo trata das várias tipologias observadas a partir dos casos identificados e aqui apresentados. Existem 52 casos a paritir de sete tipologias diferentes, conforme apresentados a seguir. As tipologias incluem: fraude com cartões eletrónicos (crédito/débito); fraude/esquema de violação de e-mail; violação e fraude dos sistemas corporativos/organizacionais; fraude através de pagamentos adiantados; fraude usando esquema Ponzi; fraude relacionada com dinheiro móvel; e casos de financiamento do terrorismo facilitados pelo ciberespaço.

Tipologia 1: Fraude com Cartões Eletrónicos (crédito/débito)

35. A partir dos casos apresentados, foram identificados 3 casos nesta tipologia. Os casos envolviam fraude eletrónica, roubo de detalhes de cartão de crédito/débito e aliciamento de vítimas para pagamento de produtos que não existem através de falsas ações de marketing online.

Caso 1: Fraude com Cartão de Crédito/Débito e o uso da Empresas de Fachada

Uma fonte apresentou uma queixa à UIF-L alegando fraude eletrónica e branqueamento de capitais por parte da Korlane Investment Limited Liability Company e dos seus proprietários corporativos. Uma investigação completa sobre a alegação foi realizada pela AAL. Os investigadores descobriram que a Korlane Investment Limited Liability Company operava uma empresa de fachada na Libéria sem escritório, sem pessoal, etc., e abriu e usou suas contas na Libéria para branquear, ocultar e direcionar fundos roubados gerados através de transações incomuns de fraude eletrónica – um crime subjacente ao branqueamento de capitais. Os suspeitos foram indiciados por branqueamento de capitais, roubo de propriedade, fraude eletrónica e conspiração criminosa.

Após obter um mandado de prisão pelo Ministério Público, os perpretadores escaparam de ser presos e fugiram do país. Foi apresentada uma moção para confisco dos produtos em conformidade com a Lei de 2013 relativa aos Recursos Provisórios dos Produtos de Crimes. A moção foi designada para audiência e discutida. O Tribunal deferiu a moção e ordenou que os produtos em mais de 234,000USD fossem confiscados e transferidos para o GOL. A técnica utilizada pelo cibercriminoso foi o uso da plataforma de E-Money Credit Card (swift, Visa e MasterCard) para realizar transações de forma fraudulenta. O criminoso manipulou o cartão MasterCard para ultrapassar o limite bancário. Tal esquema usado é conhecido como uma fraude de cartão de crédito internacional que não está em conformidade com os padrões da MasterCard.

Fonte: Libéria

Caso 2: Fraude com Cartões de Crédito/Débito e Operação Falsa de Importação/Exportação

O arguido, proprietário de uma empresa de produtos agrícolas e alfaias agrícolas, movimentava quatro contas num determinado banco. Entre 24 de janeiro de 2017 e 31 de março de 2017. O arguido, que estava envolvido em fraudes com cartões de crédito, criou um site de marketing online, através do qual recebia várias encomendas, maioritariamente dos EUA, para o fornecimento de produtos agrícolas. O arguido inscreveu-se na plataforma de pagamento online do banco, que permite aos clientes desavisados efetuar pagamentos diretamente na conta dele pelos bens en-

comendados. Em dois meses, o acusado recebeu 1,468,447,59 Ceddis ganês (USD341,500) na sua conta a partir de vários cartões de crédito de diferentes jurisdições. No entanto, o seu banco recebeu estornos da Visa e MasterCard do Bank of America de que alguns dos pagamentos feitos à empresa não eram autorizados pelos proprietários dos cartões e, portanto, fraudulentos. Durante diligências realizadas pelo banco, o arguido alegou que os fundos eram proventos da exportação de produtos agrícolas que tinha enviado através de agências de navegação para clientes.

No entanto, as investigações revelaram que as agências de navegação mencionadas não tinham enviado esses produtos e que as faturas de transporte aéreo de carga apresentadas para apoiar as suas alegações eram todas falsas. Como resultado, foi apresentada à UIF uma comunicação de operação suspeita (COS). O arguido, insatisfeito com a decisão do banco de reter os fundos, denunciou o banco à EOCO por deter os seus fundos sem justificação. Sem que o arguido soubesse, a EOCO já tinha recebido informações estratégicas da UIF para investigar o arguido. A investigação da EOCO colaborou com o FBI e a SFO para contactar as vítimas e um caso *prima facie* foi estabelecido contra o acusado que indicou que os cartões de crédito a partir dos quais os pagamentos foram feitos ao acusado eram cartões roubados.

Consequentemente, o arguido foi acusado de evasão fiscal, branqueamento de capitais e defraudação com falsos pretextos. Durante a acusação, cinco das vítimas testemunharam através de videoconferência via Skype para confirmar que, de facto, não tinham comprado bens ao arguido e que os seus cartões de crédito foram utilizados de forma fraudulenta. No final da acusação, o arguido foi condenado a uma multa de 1000 unidades de pena que é de 12,000 Ceddis ganês (USD2,390) ou, na ausência do pagamento, 5 anos de prisão.

Fonte: Gana

Estudo de Caso 3: Roubo de Cartões de Crédito/Débito e Falsificação de Identidade

Uma companhia telefónica, para melhorar os seus serviços, optou por transações internacionais de uma conta bancária para uma conta eletrónica. Esta inovação recebeu uma resposta favorável e permitiu à empresa registar bons resultados. No entanto, a empresa recebeu um alerta a informar da existência de transações internacionais fraudulentas, que foram realizadas de França para a Cote d'Ivoire. O caso foi comunicado ao órgão responsável pelo combate ao cibercrime (PLCC) com o objetivo de deter os responsáveis. Da investigação aberta na sequência do relato, conclui-se que, após a receção dos depósitos ilícitos, os números de beneficiários efetuam imediatamente os levantamentos.

As investigações realizadas pela PLCC em colaboração com o Laboratório Forense Digital levaram à descoberta dos suspeitos através dos seus números de telemóvel. O primeiro suspeito AAJ foi detido com a ajuda de uma unidade da referida empresa. Durante o interrogatório, ele admitiu ter recebido vários depósitos em dinheiro da França para a sua conta. Disse ainda que um dos seus correspondentes que conheceu no Facebook lhe pediu para fazer levantamentos de dez por cento (10%) dos montantes levantados. Ele terminou especificando que este correspondente Fabino não lhe deu quaisquer detalhes, e que apenas teve de levantar o dinheiro e entregá-lo a algum parente familiar. Investigações adicionais levaram à prisão do Senhor Fabino em sua casa em Abidjan. A busca levou à descoberta de vários cartões de crédito/débito associados a bancos de França, e que não pertenciam a Fabino. Após novo interrogatório, Fabino declarou que era responsável por ter feito 16 depósitos num montante total de 2,290,344 FCFA, ou 3,524 euros enquanto estava em França, para os números do seu amigo AAJ. Fabino era também responsável por vários levantamentos que fez da conta bancária francesa. O caso ainda estava em curso na altura da elaboração deste relatório.

Fonte: Cote d'Ivoire

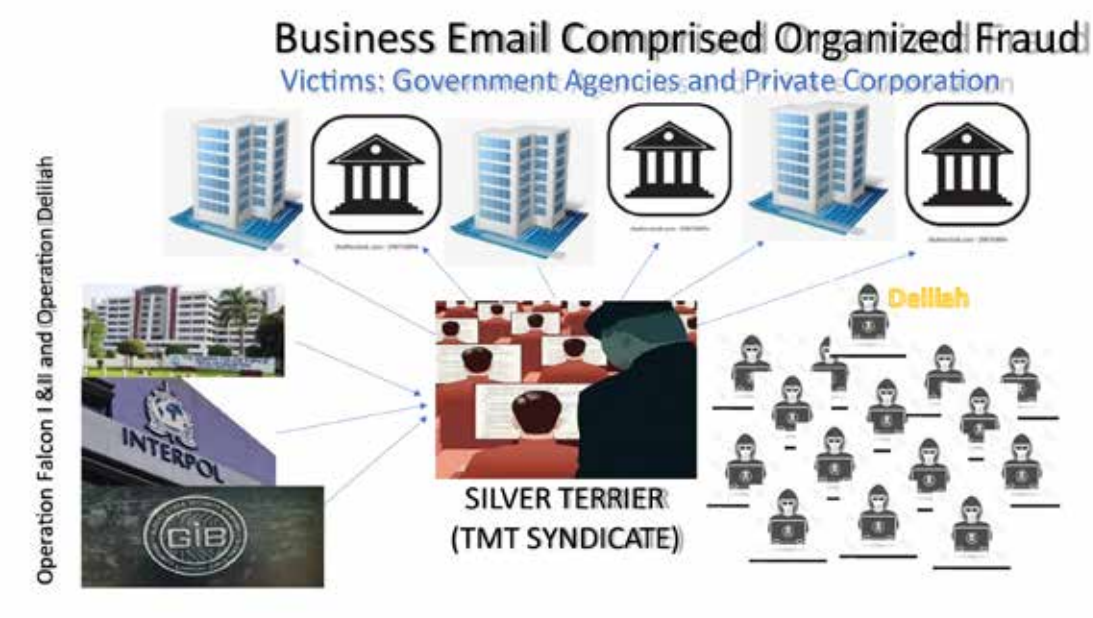
Tipologia 2: Fraude / Esquema de Violação de caixa de correio eletrónico

36. Esta tipologia está em prática há algum tempo e é muito popular na África Ocidental. Os criminosos usavam software de engenharia para ajudá-los a enviar e-mails falsos para potenciais vítimas por todo o mundo. Uma vez que você clica nesses e-mails e/ou começa a se comunicar com eles, eles podem ter acesso a informações sensíveis sobre o seu e-mail e negócio, enquanto usam essas informações para fraudar ou enganar você e os membros imediatos da sua rede.

Caso 1: Fraude organizada de Violação de caixa de correio eletrónico comercial

A Força Policial da Nigéria (NPF) deteve 11 alegados membros de uma prolífica rede de cibercrimes no âmbito de uma operação policial nacional coordenada com a Interpol. Detidos por agentes da Unidade de Polícia de Cibercrime da Polícia nigeriana e do Gabinete Central Nacional (NCB) da Interpol na Nigéria, pensa-se que muitos dos suspeitos sejam membros da "SilverTerrier", uma rede conhecida por esquemas de violação de caixa de correio eletrónico comercial (BEC) que já prejudicaram milhares de empresas em todo o mundo. A Operação Falcon II, que durou dez dias (13 a 22 de dezembro), contou com o destacamento de 10 agentes do PFN destacados da sede de Abuja para Lagos e Asaba, a fim de deter suspeitos identificados antecipadamente com informações fornecidas pela Interpol. As operações no terreno foram precedidas por uma fase de intercâmbio e análise de informações estratégicas, onde a Nigéria usou a rede global segura de comunicações policiais da Interpol, I-24/7, para trabalhar com as forças policiais em todo o mundo também investigando esse tipo de esquemas BEC ligadas à Nigéria. O Secretariado-Geral da Interpol apoiou as operações no terreno 24 horas por dia, 7 dias por semana, extraindo e analisando forensemente os dados contidos nos computadores portáteis e telemóveis apreendidos pela polícia NPF durante as detenções. Esta análise preliminar indica que o envolvimento coletivo dos suspeitos em esquemas criminosos de BEC pode estar associado a mais de 50,000 alvos. Um dos suspeitos detidos estava na posse de mais de 800,000 credenciais de domínio de potenciais vítimas no seu computador portátil. Outro suspeito monitorava conversas entre 16 empresas e seus clientes e desviava fundos para o "SilverTerrier" sempre que as transações da empresa estavam prestes a ser feitas. Outro indivíduo era suspeito de participar do crime de BEC em uma ampla gama de países da África Ocidental, incluindo Gâmbia, Gana e Nigéria.

Fonte: Nigéria



Métodos e técnicas

- Desenvolvimento de nomes de domínio, links de phishing e campanhas massivas de envio de correios eletrónicos.
- Desenvolvimento/adquisição de programas de malware/spyware e ferramentas de Acesso Remoto.
- Envolvimentto em roubo de identidade, falsificação de identidade e falsificação de documentos.
- Utilização de empresas terceiras para movimentar e desviar fundos extorquidos às vítimas.
- Uso de negócios de fachada.

Sinais de alerta e Indicadores

- Operações financeiras incomuns.
- Mudança repentina no estilo de vida, de empreendedor humilde em uma start-up a viver de forma chamativa e luxuosa.
- Fundos recebidos numa conta com nome de beneficiário diferente do nome da conta.

Caso 2: Phishing e fraude de e-mails

A investigação policial estabeleceu que a queixosa em 1 de dezembro de 2021 conta de e-mail Wawo-NGO em "wawoliberia@yahoo.com" foi manipulada (phishing) e um e-mail malicioso fazendo-se passar por wawoliberian@yahoo.com ("n" foi adicionado ao e-mail original) foi supostamente usado para se comunicar com seu Doador "DED" e levou a quantia de 20,500.00USD que foi transferida através do Bank-B em 15 de novembro, 2021 de um parceiro doador DED e também usou um número Orange (0775000...) no WhatsApp em uma conversa supostamente pretendia ser o oficial de programa da ONG Wawo, que se apresentou como oficial financeiro e um número de telefone celular 0777028... atribuído a uma conta de dinheiro móvel com nome de usuário "BM-1" foi anexado à conta de e-mail Wawo-NGO, que foi posteriormente removido após conceder acesso à conta de e-mail da Wawo-NGO. A técnica utilizada foi hackear (Phishing) a conta de e-mail e enviar e-mails maliciosos falsos a doadores pedindo fundos. Um e-mail comprometido foi alegadamente usado para solicitar fundos ao doador "DED" e configurar outros links de comunicação (WhatsApp) para autenticar a transação. O *hacker* conseguiu a mudança da conta bancária de Banco-A para o Banco-B. O esquema de branqueamento de capitais, neste caso, era a Falsificação e o Roubo de Bens. Os tipos de pessoas envolvidas eram funcionários da ONG Wawo-e um *hacker* desconhecido. Este caso está a ser investigado desde 28 de dezembro de 2021.

Fonte: Libéria

Caso 3: Fraude de violação de e-mail comercial e falsificação de identidade

A Unidade de Cibercrime da Força Policial da Nigéria, domiciliada com o Escritório Central Nacional da Interpol NCB em Abuja, recebeu um relato do governo alemão através do gabinete do Procurador-Geral e do Ministro da Justiça, relatando uma fraude de violação de e-mail comercial em ligação com a aquisição de máscaras de proteção da COVID-1 9. 'Os infratores não identificados ganharam a confiança de um intermediário na Irlanda ao iniciarem transações comerciais envolvendo produtos médicos. Ao negociar habilmente com o intermediário e apresentar contratos de entrega e faturas falsificados, os infratores fizeram o intermediário acreditar que seria capaz de entregar grandes quantidades de máscaras de proteção contra a COVID-19 para a autoridade do governo alemão. No final, foram efetuados adiantamentos no valor de mais de 2,3 milhões de euros para uma conta bancária nos Países Baixos e pagamentos parciais de 498,000 euros já tinham sido transferidos para uma conta bancária de primeira geração na Nigéria, por instrução de um nigeriano, Babatunde Adesanya, vulgo Teddy A, que deu instruções antecipadamente sobre o que fazer com o dinheiro. A Musterpoint Investment Nig Ltd., uma empresa domiciliada num banco de primeira geração na Nigéria, foi o destino dos referidos 498,000 euros. No entanto, por causa da cooperação internacional da polícia após a receção do relato, o banco foi contactado pela Interpol e a transferência foi interrompida, sendo que o dinheiro foi devolvido ao seu ponto de envio. Isto levou à detenção de dois suspeitos pela Unidade de Cibercrime da Força Policial da Nigéria, que estão agora a ser processados no Supremo Tribunal Federal da Nigéria.

Fonte: Nigéria

Caso 4: Fraude de violação de e-mail comercial

Nos dias 5 e 12 de fevereiro de 2018, um banco comercial efetuou duas transferências, respetivamente, de 50,000 Euros e 145,000 Euros a favor de duas (02) empresas. Estas transferências foram consideradas autorizadas por um dos seus clientes que tem um contrato de banca eletrónico com o banco e sempre deu instruções para as suas transferências por e-mail. O banco recebeu as instruções por e-mail para as duas transferências em questão e recebeu outro e-mail através do qual o cliente alterou os dados bancários dos beneficiários. Os vários Swifts das duas transferências foram produzidos e foram-lhe enviados após a execução. As transferências só foram contestadas em 20/02/2018, quando o verdadeiro cliente veio dizer que, embora tivesse autorizado as transferências, não tinha, no entanto, dado qualquer instrução para modificar os dados dos destinatários dos fundos da transferência. Mais tarde, o banco descobriu que um cibercriminoso tinha conseguido aceder ao sistema do banco e introduzira essas modificações de destinatários com e-mails falsos no processo de transferência. O caso ainda estava em curso no momento deste relato).

Fonte: Togo

Caso 5: Fraude de violação de e-mail comercial

A UIF recebeu uma denúncia de fraude de roubo de identidade da Hibiscus, uma ONG local. Estes esperavam o seu segundo desembolso de fundos de seus parceiros internacionais, Gardenia Help totalizando NLe707.841,12 destinados às principais populações afetadas no interior. Os fundos foram desviados fraudulentamente para outra conta com o mesmo nome Hibiscus noutro Bank WY. As investigações internas da Hibiscus revelaram que o e-mail do Gestor do Programa havia sido violado e era o principal canal para o fluxo de informações relevantes entre os infratores e os parceiros internacionais. As atividades de Hibiscus haviam sido suspensas pela Gardenia até que o assunto fosse resolvido.

As investigações da UIF revelaram que uma conta fraudulenta da Hibiscus foi de facto aberta no Banco WY e que os fundos no total de NLe707,841,12 foram, de facto, transferidos diretamente da Gardenia Help.

Os fundos foram imediatamente transferidos para outra conta Sunflower Tech dentro do mesmo banco e levantados no prazo de três dias pelo único signatário da Sunflower Tech. As investigações também revelaram que havia uma ligação direta entre o fraudulento Hibiscus NPO, Sunflower Tech e seu signatário. O Banco WY não realizou as devidas diligências e medidas KYC durante a abertura da conta fraudulenta da Hibiscus. Se o tivessem feito, teriam detetado todos os sinais de alerta gritantes. Estavam mais preocupados com a rentabilidade.

A ONG Gardenia Help e a ONG Hibiscus têm um conhecimento muito limitado de branqueamento de capitais e financiamento do terrorismo, tornando os seus sistemas internos porosos e facilmente suscetíveis a infratores dentro das suas organizações. O beneficiário final foi detido pelo CCA e as investigações estão em curso.

Fonte: Serra Leoa

Tipologia 3: Pirataria informática e defraudação dos sistemas corporativos/organizações (website/base de dados)

37. Outra tipologia popular é violar *hackear* e assumir o site ou plataforma/banco de dados corporativo usando técnicas de engenharia e software muito sofisticados. As técnicas não são muito diferentes dos ataques de Malware ou Ransomware. No entanto, na África Ocidental, os criminosos dificilmente se revelam pedindo resgate. Eles são pagos para isso por rivais ou concorrentes ou, no caso de instituições financeiras, a plataforma onde as transações são feitas é assumida e controlada para executar transferências e pagamentos ilegais antes que as vítimas possam detetar e fazer esforços para recuperar o controlo do seu sistema. Há momentos em que o abuso de informação privilegiada faz parte do modus operandum.

Caso 1: Violação de Sistemas Corporativos (Distribuição de Negação de Serviços ou fraude)

Um cibercriminoso britânico, Sr. Kaye atacou uma empresa liberiana GSM e inadvertidamente fez colapsar a internet na Libéria - em 2016. Kaye, de Egham em Surrey, é um *hacker* autodidata que começou a vender as suas habilidades consideráveis na *dark web* (submundo da internet) - oferecendo aos indivíduos oportunidades de atacar e destruir seus rivais nos negócios. De acordo com documentos judiciais, Kaye foi contratado em 2015 para atacar uma empresa líder de telefonia móvel e provedor de internet, por um indivíduo que trabalhava para sua rival e principal concorrente. Não havia nenhuma sugestão de que a empresa rival estava ciente da ação do seu funcionário - mas o indivíduo ofereceu a Kaye até 10,000 USD (R£ 7.800) por mês para usar as suas habilidades para destruir a empresa, causando descrédito e danos à reputação.

Os utilizadores de telemóveis começaram a ver os seus dispositivos ficarem *offline* – sem rede à internet. A empresa chamou consultores de segurança cibernética que tentaram repelir o ataque, mas a essa altura já era tarde demais porque a *botnet* (rede de bots) estava descontrolada. A Internet da Libéria dependia de um pequeno número de fornecedores e de um cabo atlântico relativamente limitado. Kaye havia enviado tanto tráfego para a empresa, fazendo com que todo o sistema cibernético nacional ficasse congestionado. Segundo os investigadores, a internet do país falhou repetidamente entre 3 e 4 de novembro de 2016 - perturbando não apenas a empresa que foi atacada, mas organiza-

ções e pequenas empresas e usuários individuais em todo o país. Por sua vez, as ações de Kaye impediram os clientes da empresa de comunicarem entre si, de obterem acesso a serviços essenciais e de realizarem as suas atividades comerciais quotidianas. Um número substancial de clientes mudou para o principal concorrente.

Kaye admitiu a acusação de um crime de uso indevido de computador, lançar ataques cibernéticos contra uma empresa na Libéria e estar na posse do produtos do crime - relativo aos 10,000 USD encontrados na sua pessoa quando foi preso. Nos anos anteriores aos ataques de distribuição de negação de serviço (DNS), a receita anual da empresa havia ultrapassado 80 milhões USD (R£ 62,4 milhões). As receitas pós-ataque registaram uma diminuição de dezenas de milhões e um aumento do passivo da empresa, também em dezenas de milhões de dólares.

Fonte: Libéria

Caso 2: Violação de Sistemas Corporativos (DNS ou fraude)

Em 2020, uma instituição financeira denunciou à polícia de que cibercriminosos haviam comprometido (violado) todo o seu sistema bancário e tiveram acesso total ao seu sistema bancário central. Os cibercriminosos modificaram os números de referência das transações e injetaram uma soma total de D48.000.000 (USD 857.142,8) em diferentes contas. Os piratas informáticos também retiraram o limite de levantamentos diários nos ATMs do banco, permitindo assim que os titulares das contas (atores/conspiradores/cúmplices locais) levantassem o máximo possível. Os piratas informáticos executaram consultas no sistema bancário e apagaram todos os históricos de transações ilegais e, como resultado, as transações nas contas afetadas não podiam ser visualizadas usando o *front-end* do banco, mas só podiam ser visualizadas a partir do Servidor do interruptor Gam no banco central.

O titular da conta (atores locais/conspiradores/cúmplices) conseguiu sacar (usando caixas eletrónicas) D7.000.000 (USD 125,000) e uma investigação mais aprofundada revelou que parte do dinheiro foi enviada para Gana, África do Sul e Senegal. No entanto, através da cooperação internacional (Interpol e UIF), parte dos fundos enviados para o Gana foi recuperada a partir de uma conta corporativa e todos os fundos enviados para o Senegal também foram recuperados.

Além disso, é importante reconhecer que, na época desta investigação, o país não tinha um laboratório forense digital para examinar os dispositivos. Apesar de nenhum dos piratas informáticos ter sido detido, foram detidos 23 suspeitos, cúmplices/conspiradores dos piratas informáticos. A investigação foi concluída e o caso foi encaminhado à Procuradoria-Geral da República para aconselhamento.

Fonte: Gâmbia

Caso 3: Violação de Sistemas Corporativos (DNS ou fraudae)

Durante o mês de julho de 2020, a Brigada Central de Luta contra Cibercrimes recebeu uma instrução, através de uma carta enviada pelo Procurador da 1ª Vara do Supremo Tribunal de Uagadugu, para realizar uma investigação detalhada sobre acesso fraudulento e obstrução ao funcionamento de um sistema informático, modificação de dados informáticos, associação ou acordo para cometer infrações informáticas, roubo de dinheiro, branqueamento de capitais e para apresentar acusações contra qualquer pessoa envolvida nos crimes acima mencionados.

A investigação revelou que, na noite de domingo, 21 de junho, para segunda-feira, 22 de junho de 2020, piratas informáticos atacaram uma plataforma eletrónica de dinheiro móvel através de uma rede telefónica. Atacaram cinco (05) contas principais da plataforma e a conta de um banco local onde a plataforma de dinheiro móvel estava alojada e era gerida. Os piratas informáticos realizaram transferências fraudulentas no valor total de noventa e nove milhões cento e oitenta e sete mil quinhentos e setenta e nove (99,187,579) FCFA. Estas transferências foram feitas para vários números de telefone, titulares de contas de dinheiro móvel no país e para outros números em 3 outros países vizinhos. A soma total de dinheiro nas contas que os piratas informáticos conseguiram bloquear, tanto nacional como internacional, foi de mais de trezentos e oitenta e um milhões (381,000,000) FCFA.

A investigação permitiu a prisão de vários suspeitos e foram levados ao Ministério Público da 1ª Vara do Supremo Tribunal para providências complementares.

Fonte: Burkina Faso

Caso 4: Branqueamento (Circulação) através de um Funcionário Bancário Comprometido

De 20 a 29 de setembro de 2022, um banco comercial em Bissau denunciou que indivíduos desconhecidos tinham realizado algumas operações fraudulentas de transferência *online* e que não eram funcionários do banco. Segundo fontes da UIF e da Polícia, as transferências foram feitas da própria conta do banco para as contas dos clientes no mesmo banco.

Na sequência da investigação, a PJ, com o apoio da Unidade de Conduta Criminosa e Burla e da Unidade Nacional de Combate a Crimes Económicos, solicitou a colaboração das empresas de telecomunicações para rastrear as comunicações efetuadas no último mês, utilizando determinados números (6 números SIM) suspeitos de estarem envolvidos no caso. A Sra. Y, a 1ª suspeita, cooperou com a Polícia quanto ao seu envolvimento na conduta criminosa de fraude e quebra de confiança.

A Sra. Y confessou que é titular de uma conta poupança domiciliada no Banco XPTO em Bissau, no entanto, a pedido do seu marido Sr. X, forneceu o seu número de conta a um amigo Mário, que precisava de uma conta ligada a um cartão VISA no Banco XPTO. Sem qualquer devida vigilância, o Sr. X forneceu os detalhes da conta ao seu amigo Mario. Poucos dias depois, a Sra. Y aludiu ao facto de ter recebido uma mensagem no seu telemóvel a indicar uma operação de crédito no valor de seiscentos e quarenta e oito mil, cento e quarenta e um francos CFA (648,141 CFAF). Mais tarde, ela disponibilizou o seu cartão de débito VISA ao marido, que através do amigo, recolheu o dinheiro em prestações.

E dias depois, a conta foi novamente creditada com a soma de cinco milhões de francos CFA (5,000,000 CFAF). Desta vez, o amigo do marido pediu-lhe para ir ao balcão do banco fazer um levantamento direto, que deveria ser através de aviso prévio, mas devido à relação do marido com um dos funcionários, ela conseguiu levantar o valor total de uma só vez. Mais tarde, ela recebeu uma chamada de KP, que lhe pediu para regressar ao banco a fim de esclarecer a situação em relação ao levantamento indevido que fez e das anomalias que ocorreram na sua conta.

A investigação ainda está em curso. No entanto, vale a pena notar a existência de falhas no sistema de controlo de transferências de dinheiro eletrónico no banco referenciado e que os criminosos cibernéticos, em colaboração com certos funcionários do banco, aproveitaram para realizar transferências ilegais fora do funcionamento normal do banco. O caso revelou ainda as vulnerabilidades do sistema de controlo ao nível dos bancos e instituições financeiras, bem como as ameaças de cibercrime que o país enfrenta, nomeadamente, na ausência de infraestruturas e capacidades técnicas para fazer face a essas ameaças.

Fonte: Guiné-Bissau

Caso 5: Violação de conta na rede social, burla (falsa identidade) e fraude

A vítima Mary T. relatou à polícia que alguém que se passava por seu tio através da sua conta de Messenger no Facebook e lhe pediu para transferir 800.00 USD e LR$ 75,000.00 para um determinado número a 11 de maio de 2022. O pirata informático criou uma conta Messenger no Facebook usando o nome completo do tio. A ideia era de que o tio precisava urgentemente de dinheiro para liquidar algumas obrigações na Libéria e o dinheiro ser-lhe-ia devolvido posteriormente. Depois de ser convencida e com base na confiança que tinha no tio, ela fez uma transferência do montante dos EUA via MoneyGram, conforme instruído. O criminoso, após violar a conta do menssenger do tio da vítima e se fazer passar pelo tio, solicitou a transferência de dinheiro e enviou uma mensagem instruindo a vítima a transferir dinheiro para um determinado número. Os crimes subjacentes ao branqueamento de capitais são fraude

e extorsão/roubo de bens perpetrados por um indivíduo e um pirata informático desconhecido. Neste caso, a vítima recebeu mensagem supostamente do tio para transferir fundos para a conta de dinheiro móvel. O caso está a ser investigado.

Fonte: Libéria

Caso 6: Uso de informação privilegiada, Esquema de facilidades de crédito organizado e fraudulento

A UIF recebeu uma denúncia (Investigação Fraude-Retorno) sobre um Desembolso de Crédito Suspeito Não Autorizado do Jimpex Commercial Bank (JCB). 150 clientes do JCB receberam facilidades de descoberto, de forma fraudulenta, sem documentação, no valor de Le54.484.754.082,47 (0,5 milhões de dólares americanos).

O Responsável de Seguimento das Carteira da JCB e o Chefe Interino de Divisão (Gestão de Risco de Crédito) foram os mentores desse esquema ilegal. Em seguida, envolveram no esquema pessoal de informático (TIC) que tinha acesso aos dados.

O Gestor de Risco de Crédito utilizou o seu código de acesso especial para autorizar montantes a descoberto a clientes pré-selecionados da JCB. O Gestor de Risco de Crédito selecionou cuidadosamente os clientes existentes do banco que operavam negócios credíveis e aliciou-os a envolverem-se no esquema ilegal. Cada um dos beneficiários do esquema ilegal foi solicitado a que fornecer uma determinada quantia em dinheiro aos conspiradores antes que eles pudessem ter acesso à facilidade de descoberto ilegal. Após o pagamento do valor solicitado, o Gerente de Risco de Crédito autorizou a facilidade *montante a descoberto* utilizando o seu código de acesso. O pessoal das TIC que fazia parte do esquema também fechou os olhos.

A investigação da TOCU ligou 4 casas ultramodernas recém-construídas e uma frota de carros de luxo ao gestor de risco de crédito e ao responsável pelos relatórios de carteiras. O gestor do risco de crédito está em fuga e as investigações estão em andamento.

Fonte: Serra Leoa

Tipologia 4: Fraude de Pagamento Adiantado e Branqueamento de Capitais

38. Este é ainda o crime subjacente facilitado pela cibernética mais cometido na África Ocidental. Representa mais de 40% dos casos aqui relatados. O adiantamento de taxas basea-se num esquema romântica, extortion sexual, reivindicações de herança ou propostas comerciais, ou uma combinação de dois ou mais dos métodos mencionados. Outro método que merece ser destacado é a fraude de pagamento adiantado realizada a partir das grades da prisão, tendo funcionários penitenciários como cúmplices.

Caso 1: Esquema usando Ouro e Fraude de Pagamento Adiantado

Este caso foi investigado pela polícia com base numa queixa apresentada por dois empresários britânicos. Os dois investidores do Reino Unido e seus parceiros de negócios foram apresentados em 2020 por um conhecido *online* ao Sr. 'A', um ganês, como sendo um empresário negociante de ouro. Os investidores manifestaram interesse em comprar barras de ouro do Sr. 'A' e, posteriormente, viajaram para Gana, a convite do Sr. A, que também exigiu que o encontrassem pessoalmente para negociarem a transação. Em fevereiro de 2020, o Sr. 'A' e um cúmplice, o Sr. B, encontraram-se com os investidores e mostraram-lhes 20 quilos de barras de ouro.

Os investidores estrangeiros expressaram sua disponibilidade para comprar cinco quilos do ouro, pelos quais o Sr. 'A' e seu cúmplice exigiram e receberam 69,000 USD como pagamento inicial e parcial do valor do ouro. Após receberem o dinheiro, eles prometeram exportar o ouro para os investidores, que os receberiam em Dubai, nos Emirados

Árabes Unidos. Mas acabaram por exportar apenas um quilograma de ouro para os investidores. O Sr. A' explicou que não podia exportar a quantidade adequada de ouro devido a atrasos no processo de documentação por parte dos funcionários aduaneiros no Aeroporto Internacional de Kotoka e prometeu exportar a quantidade restante para os investidores a 3 de dezembro de 2020, mas não o fez. Mais tarde, ele pediu 130,000 USD, o pagamento remanescente dos os quatro quilos de ouro e solicitou outros 70,000 USD dos investidores para garantir a exportação do resto do ouro. Quando não honrou a sua palavra, indicou que não tinha podido exportar o ouro, uma vez que não havia companhias aéreas para fazer a exportação do ouro devido à pandemia de COVID-19.

O Sr. A também alegou que a carta de porte para facilitar a exportação do ouro não poderia ser aceite pela Precious Minerals Marketing Company, pois a quantidade era muito pequena, então ele adicionaria cinco quilos adicionais de ouro para aumentar o total para 10 quilos a fim facilitar a exportação. Em julho de 2020, O Sr. A disse aos investidores que tinha sido preso pela Interpol e funcionários de algumas agências de segurança e que as barras de ouro tinham sido confiscadas.

Para facilitar a libertação do ouro, exigiu várias quantias em dinheiro e, mais tarde, indicou que as barras de ouro tinham sido libertadas para o Gabinete de Crimes Económicos e Organizados (EOCO), que exigia 300,000 dólares antes de libertarem o precioso mineral. Os investidores enviaram os 300,000 USD para o Sr. A, elevando o valor total enviado para 1,075,000 USD, mas ele não cumpriu a promessa, levando à sua prisão. Foi então acusado de conspiração para cometer fraude sob falsos pretextos, defraudar com falsos pretextos e venda e compra de minerais sem licença. O julgamento está atualmente em curso.

Fonte: Gana

Caso 2: Extorção sexual, pornografia infantil e extorsão

Em 2016, foi denunciado à polícia um caso de três indivíduos: Flávio, Filipe e Steve. Os suspeitos criaram um perfil falso nas redes sociais com o nome de "Maurice Marcovich", usado para fins criminosos. Eles usaram a página falsa para enviar pedidos de amizade para suas potenciais vítimas, que eram, na sua maioria, menores de idade no momento do crime. Depois de trocarem algumas mensagens no bate-papo através do Messenger no Facebook, começaram a ameaçar de morte as vítimas, suas famílias e/ou entes queridos se não se mostrassem em poses pornográficas, tirando fotografias e fazendo vídeos com os seus próprios telemóveis e forçando-as a enviá-los através do Messenger.

Tendo visto as fotografias e filmagens das vítimas durante as conversas via bate-papo na Internet –Messenger, o "perfil falso" sob o nome de "Maurice Marcovich", ordena às vítimas que enviem um pedido de amizade a "Flávio Yolo Alves", "Rui Filipe Alves" e "Steve Aristides Santos", no Facebook.

Ainda através deste artifício, assustavam e coagiam as vítimas a encontrarem-se com eles e a praticarem atos sexuais, filmando com os seus telemóveis, e com os das vítimas, o que aceitavam devido ao medo que lhes incutiam, quer através de ameaças, quer através da ameaça de divulgação pública das suas fotografias e vídeos pornográficos que já possuíam.

As vítimas foram ameaçadas, não só com a publicação de fotografias e vídeos, mas também com o envio de uma foto de uma arma de fogo a ser carregada com as seguintes mensagens: "não vais mais ignorar-me", "mato todos os dias", "sei muito sobre ti", "porque quero o teu sangue", "amanhã pode ter certeza que não vai ter vida", "sou traficante internacional de drogas na Síria, Brasil e França", "e já ordenei o assassinato de vários estudantes no Iraque" sic. Eles também enviaram às vítimas fotos de seus parentes, feitos em locais públicos e perto de suas casas, para intimidá-las e assustá-las ainda mais.

Perante estas insistentes ameaças de morte, as vítimas, desesperadas e com medo, acederam às pretensões destes indivíduos, e enviaram mais fotografias e vídeos, obscenos e indecentes, mostrando as suas partes íntimas, bem como os seus rostos.

Estes indivíduos, por vezes individualmente ou em grupo, combinaram encontrar-se com as vítimas em locais diferentes, obrigando-as a ter relações sexuais com elas, e os atos foram filmados e fotografados, alegando que tinham ordens de "Maurice Marcovich" para fazer tudo aquilo e enviá-los.

No decurso destes atos violentos contra estas vítimas, uma delas, menor de 13 anos, engravidou, e posteriormente foram recolhidas provas, que se basearam na recolha de ADN dos suspeitos para efeitos de identificação da paternidade, que comprovaram que "Rui Filipe Alves" era o pai.

Insatisfeitas com as ações acima referidas, continuam sob constante ameaça, recorrendo ao falso perfil "Maurice Marcovich", obrigaram algumas vítimas a prostituírem-se e, em consequência, receberam o dinheiro dessa prática, que cobraram a cada cliente, uma quantia entre 5 e 7 mil contos, aproximadamente 50 a 70 euros/dólares.

Os indivíduos "Flávio Yolo Alves" e "Rui Filipe Alves" foram detidos e apresentados em tribunal e quando julgados, Flávio foi condenado a 33 anos de prisão e Rui a 14 anos.

Fonte: Cabo Verde

Caso 3: Uso de empresa fictícia/de fachada e Fraude de pagamento adiantado

Em 2009, o Sr. A, um comerciante, abre uma conta no banco X por motivos relacionados com as suas atividades comerciais. Mas, nesta conta ele só recebe transferências do exterior. Quatro anos depois (2013), a sua mulher abriu uma conta no mesmo banco, novamente por motivos comerciais. Esta última conta recebeu, no período de 2013 a 2019, 48 transferências num total de 122 282 518 FCFA. Apenas foi efetuada uma operação de pagamento na conta. Mas, surpreendentemente, o Sr. A controla a conta de sua esposa na totalidade. Todas as retiradas foram feitas por ele mesmo e, geralmente, imediatamente após cada depósito recebido. Em 2014, constituiu e abriu uma terceira conta na mesma instituição bancária. Nas mesmas condições, ele se beneficia de 114,905,014 FCFA entre 2014 e 2019. Todos estes factos levaram o banco X a fazer uma comunicação de operação suspeita à CENTIF. Em 2018, ele abriu outra conta num segundo banco Y e recebeu uma transferência de um banco nigerino, num montante total de 189,500,000 FCFA, que se revelou uma transferência fraudulenta obtida a partir de um ataque ao sistema informático do banco. Mas, graças à vigilância feita a esta última, os fundos puderam ser devolvidos antes do Sr. X entrar na posse dos montantes. O Banco Y envia imediatamente uma COS para a CENTIF. As investigações da CENTIF revelaram que o Sr. X é o irmão mais novo de um criminoso cibernético conhecido nas bases de dados. Ele faz parte de uma rede de criminosos cibernauticos que se envolvem em golpes ao estilo nigeriano (golpe 419). Seu método é o uso de empresas de fachada e intermediários ou seus indicados para atrair suas vítimas, oferecendo-lhes negócios muito lucrativos. No decorrer da relação, eles criam custos imaginários que a vítima deve pagar, em particular os custos de estudo do processo, honorários de advogados, honorários de contabilistas, etc. Tudo isso, permitiu-lhes extrair 451,615,304 CFA das vítimas. Na sequência das investigações, o Sr. X foi considerado culpado de branqueamento de capitais, fraude organizada e violação da segurança informática e condenado a 72 meses de prisão, 12 dos quais foram suspensos, e a uma multa de 100,000,000 CFA. Sua esposa foi condenada por branqueamento de capitais simples, na sua forma menos gravosa, e sentenciada a 36 meses de prisão, 12 dos quais suspensos, e a pagar uma multa de 50,000,000 CFA. Houve confisco de 11,481,787 FCFA apreendidos em uma de suas contas e confisco de um carro que lhes pertencia em benefício do Estado.

Fonte: Togo

Caso 4: Fraude Romântica e Fraude de Pagamento Adiantado

O Sr. A, um cidadão ganês que se fez passar por mulher para defraudar um cidadão australiano de 43 anos, o Sr. X, numa burla de romance, foi condenado a 10 anos de prisão. Nas suas relações com a vítima, o Sr. A fez-se passar por uma mulher com uma identidade falsa *online* e conheceu a vítima num site de encontros. A vítima é um pescador comercial reformado e cidadão australiano. A vítima indicou que, depois de se envolver com o golpista online, o Sr. A o convenceu a comprar propriedades em Gana e também a sustentar financeiramente a suposta família do Sr. A. Como resultado, ele enviou uma quantia total de 115,000 AUS para os acusados no Gana através de transferências bancárias.

A vítima, percebendo que estava a ser defraudado, apresentou queixa junto do EOCO e solicitou que o EOCO realizasse investigações ao alegado esquema de burla. O arguido foi detido em dezembro de 2017 e foi posteriormente formalmente constituído arguido pelo Tribunal de 1ª Instância pela acusação de burla com falsos pretextos, branqueamento de capitais e posse de documentos falsos. Em junho de 2018, o acusado foi considerado culpado das acusações e condenado a 10 anos de prisão com trabalhos forçados. A quantia de 52,000 Ceddis (11,000 USD) pendente na sua conta foi congelada e remetida à vítima.

Fonte: Gana

Caso 5: Fraude no recrutamento de emprego e fraude de pagamento adiantado

Em 2022, as investigações neste caso tiveram origem em várias denúncias feitas aos órgãos de polícia criminal (OPC), à Polícia Judiciária e à Polícia Nacional, onde algumas vítimas relatam que receberam um convite via rede social, FACEBOOK, de um perfil com fotografia do Ministro dos Negócios Estrangeiros e Comunidades de Cabo Verde, e outros dizem ter recebido um convite de um perfil do Vice-Ministro do Primeiro-Ministro e Ministro das Finanças ao qual aceitaram por pensar que se tratava destes senhores.

Que depois de aceite o pedido de amizade, as pessoas nos perfis começaram a trocar mensagens escritas em português, através do Messenger, e durante a conversa, prometeu-lhes uma oferta de emprego na Organização das Nações Unidas (ONU), como diplomata representante de Cabo Verde, cujo salário seria de aproximadamente cinco mil dólares por mês (aproximadamente 500,000$00 mil escudos cabo-verdianos) tendo em conta que o salário mínimo em CV é de 13,000$00 mil escudos (130 dólares USD).

Tendo feito esta promessa de trabalho e aceite pelas vítimas, a pessoa nos perfis fornece-lhes um contacto que afirma ser de um funcionário da ONU, com quem elas, as vítimas, devem começar a falar para tratar de assuntos relacionados com a contratação para o cargo.

Normalmente, esse contato é um número no WhatsApp, e as vítimas começam a falar com a pessoa que, em todos os casos denunciados, disse que era a voz de um homem. A pessoa pede-lhe que envie documentos, como uma cópia do passaporte, curriculum vitae, registo criminal e o dinheiro através de uma transferência para pagar os custos de processamento dos documentos (contratos de trabalho, crachá de identificação como funcionário da ONU, etc.,).

As vítimas enviam as quantias solicitadas via Western Union ou Money Gram, quantias de cerca de 100,000 escudos (1,000 euros), mas dias depois, essa pessoa volta a contactá-las para pedir mais dinheiro para o processo de contratação e, para dar mais credibilidade, enviam um contrato de trabalho que tem de ser assinado e enviado por email. Uma vez assinado e enviado o contrato, voltam a pedir mais valores, com outras justificações. No entanto, se a vítima se revelar incapaz de pagar, ameaça anular o contrato.

Quando as vítimas estão situação de desespero, quando já não conseguem pagar, dirigem-se pessoalmente ao Ministro ou fazem-no através de terceiros conhecidos do Ministro e, é assim que se esclarece que entraram num esquema onde foram enganadas por cibercriminosos, portanto, os perfis não pertencem aos Ministros. Por outras palavras, são falsos.

Em relação aos factos acima expostos, em que se encontram sete (07) vítimas, os cibercriminosos tiveram um rendimento no valor total de 3,387,730$00 ECV, (correspondente a 31,709,2USD). No entanto, todo o dinheiro foi enviado via Western Union, para o Benim, especificamente Cotonou.

Fonte: Cabo Verde

Caso 6: Fraude de Proposta de Negócio e Fraude de Pagamento Adiantado

Em 3 de dezembro de 2018, a CENTIF-TOGO recebeu uma comunicação de operação suspeita de uma instituição financeira, após várias transferências de fundos recebidos do exterior pelo Sr. KM. Na abertura da conta, ele declarou ser gerente da empresa ES cuja atividade é a importação-exportação de calçados e bolsas. Para uma empresa cuja vocação é a importação e exportação, os fundos devem normalmente ser enviados do Togo para países estrangeiros para comprar bens, mas não só a conta nunca fez transferências para o Estrangeiro, como tem funcionado mais como uma conta "trampolin", onde os fundos das transferências recebidas são imediatamente levantados, deixando a conta inativa até que uma nova transferência é recebida. Isso se enquadra no caso atípico de um esquema de fraude cibernética do tipo golpe 419. As investigações da CENTIF revelaram que o senhor tem outra conta ao nível de uma instituição financeira B e cuja operação é idêntica à da conta na instituição A. Em 18 de junho de 2021, a CENTIF-TG recebeu partilha de informações de sua congénere no Japão sobre o Sr. KM, pelos fatos de tentativa de fraude através de uma transferência fraudulenta. De fato, a 25 de dezembro de 2020, um cidadão japonês Sr. JJ apresentou-se nos balcões de um banco no seu país e insistiu no facto de que ele tinha 3,300,000 USD ou aproximadamente 1,980,000,000 FCFA na sua conta bancária no Togo. Esta conta acaba por ser a conta B de Sr. KM. O Sr. JJ pede então ao seu banco que transfira 400 USD para a referida conta para cobrir as formalidades para recuperar os 1,980,000,000 FCFA aí disponíveis. A instituição financeira japonesa recusou-se a executar a ordem de transferência devido a dúvidas que tinha sobre o motivo da transferência e apresentou uma COS à unidade de informação financeira do Japão que, por sua vez, comunicou o caso à CENTIF TOGO. No entanto, a vítima, foi alvo de extorção entre 2015 e 2021, e fez 41 transferências de fundos recebidos de, pelo menos 37,598,670 FCFA.

Fonte: Togo

Caso 7: Esquema de burla de Romance / Ouros e Fraude de Pagamento Adiantado

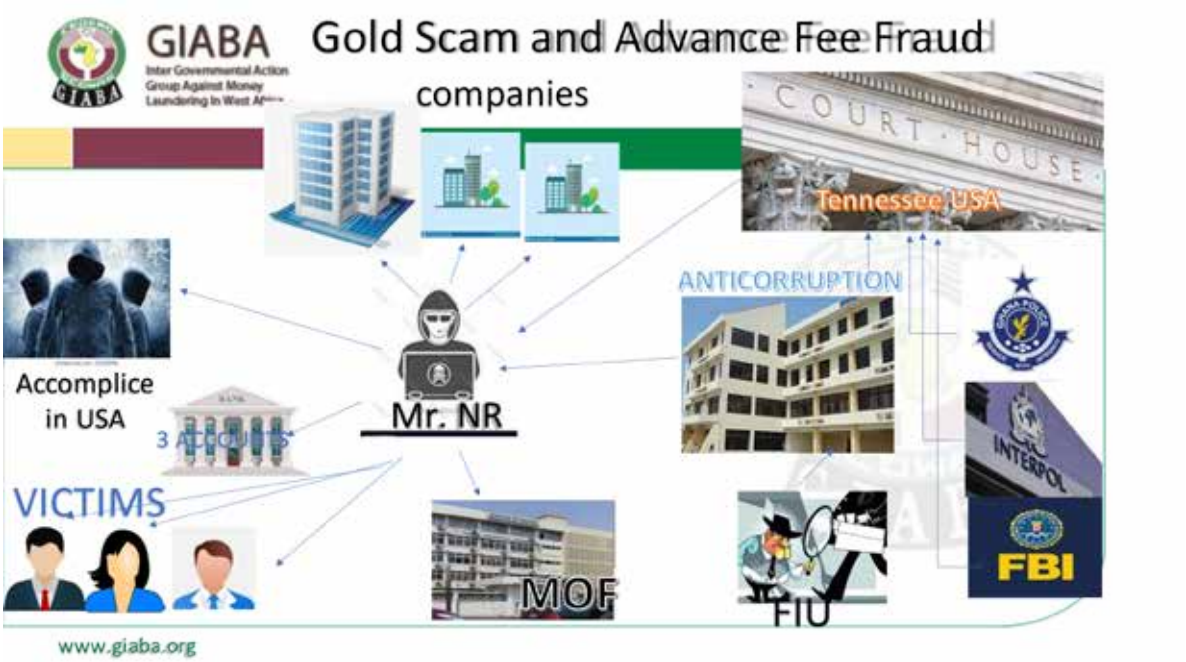
Estudo de Caso 2

Uma informação estratégica foi enviada pela UIF ao EOCO sobre as atividades de um cidadão nigeriano residente em Gana que possuía e operava uma empresa cuja sua natureza de negócios era marítimos, *bunkering*, transporte marítimo e construção. Chamou a atenção da Unidade de Informação Financeira (CIF) quando o indivíduo recebeu algunas depósitos dos EUA. Quando foi inicialmente questionado sobre esses depósitos, ele alegou que estava a tratar de criar um banco e que estava em vias de obter a aprovação do Banco do Gana. Em agosto de 2016, ele recebeu depísitos adicionais a totalizar 330,749,47 USD de três fontes, uma instituição corporativa nos EUA e dois cidadãos americanos. A sua conta bancária foi imediatamente congelada pelo EOCO, tendo sido iniciada uma investigação. Durante a investigação, foi estabelecido que ele se apresentou falsamente a algumas das vítimas que conheceu no site de namoro www.match.com como um homem branco trabalhando em projetos em Gana, com pseudônimos falsos. Ele também se apresentou erroneamente como um negociante de ouro negociando sob o nome de duas empresas falsas que supostamente tinham ouro no valor de 8 milhões USD. Também apresentou documentos falsos que supostamente emanavam do Ministério das Finanças como prova de que o seu suposto ouro estava detido no Ministério.

Em agosto de 2017, enquanto a investigação estava em curso no Gana, um grande júri federal no Tribunal Distrital dos EUA para o Distrito Ocidental do Tennessee indiciou o suspeito e outros por conspiração para cometer fraude eletrónica, conspiração para cometer branqueamento de capitais, conspiração para cometer fraude informática e roubo de identidade agravado. O tribunal federal indicou que o suspeito, em colaboração com outros coconspiradores nos EUA, utilizou técnicas sofisticadas de anonimização, incluindo o uso de endereços de e-mail falsificados e Redes Privadas Virtuais, os coconspiradores identificaram grandes transações financeiras, iniciaram correspondência fraudulenta por e-mail com partes comerciais relevantes e, em seguida, redirecionaram os fundos. As vítimas foram identificadas como sendo dos EUA, Austrália, Reino Unido e Finlândia.

Ele foi extraditado para os EUA em dezembro de 2019 e foi condenado a 3,5 anos de prisão em 16 de junho de 2021. A investigação contou com colaborações da UIF, do Serviço de Polícia do Gana, da Interpol e do FBI a todos os níveis, que conduziram uma investigação e acusação bem-sucedidas. Não foi identificada qualquer ligação ao financiamento do terrorismo. Em junho de 2022, o EOCO iniciou uma ação no tribunal para repatriar os produtos do crime, congelados nas várias contas bancárias, para os EUA.

Fonte: Gana



Métodos e técnicas

- Uso de sites populares de encontros/namoro usando identidade falsa
- Estabelecer relações *online*/à distância e criar confiança para atrair as vítimas
- Recurso a profissionais terceiros, em especial a pessoas coletivas
- Uso de empresas de fachada

Sinais de alerta e Indicadores

- Operações financeiras incomuns
- Inconsistências nas declarações durante o interrogatório policial
- Fundos recebidos na conta com nome de beneficiário diferente do nome da conta

Caso 8: Fraude de contratos comerciais (importação/exportação) e fraude de adiantamento de taxas

XZ, residente em Niamey, recebeu uma chamada telefónica (GSM) de um número, com um código de França. Seu interlocutor ao telefone, apresentando-se como GMN, havia recolhido informações específicas suficientes sobre ele a ponto de XZ acreditar que a GMN o conhecia há muito tempo. GMN consegue estabelecer e ganhar através de uma engenharia social bem lubrificada a confiança de XZ. GMN ofereceu a XZ um acordo para entregar uma das seivas de moringa. GMN explicou a XZ que tinha uma relação comercial com uma personalidade conhecida, mas falecida. XZ é, portanto, escolhido para substituir este, GMN explicou-lhe, especificando a quantidade desejada. GMN explicou a XZ que a seiva de moringa é um produto muito popular que ele está a pesquisar em nome de um médico que trabalha para um laboratório baseado na França no Carrefour KYC.

GMN comunicou a XZ o nome de Kaboré Elh Moussa, domiciliado em Uagadugu, bem como o número de telefone de BBP a partir do qual Kaboré e GMN alegaram obter fornecimentos de seiva de moringa no passado. XZ é informado de que deve entrar em contato com BBP para perguntar se ele ainda tem seiva de moringa em quantidade e qualidade e, ao mesmo tempo, perguntar sobre o preço.

Depois de XZ e BBP terem concordado com a quantidade disponível, bem como o preço, BBP ofereceu a XZ receber uma primeira amostra. Esta amostra é entregue diretamente em Niamey por uma pessoa apresentada como filho de BBP que recebe pessoalmente os custos relacionados com o preço da amostra. A amostra foi submetida à perícia de AC, um europeu cujo número de telefone tinha sido fornecido a XZ por Kaboré Elh Moussa. Uma vez confirmada a qualidade por AC, XZ e BBP acordaram as condições de entrega (custos, métodos de transporte, etc.) de toda a encomenda. Para isso, vários custos adicionais são solicitados a XZ dependendo da natureza dos bens. Estes são os custos de embalagem, fitossanitários e formalidades administrativas, incluindo as alfândegas.

Depois de todos estes encargos, incluindo o preço de compra da encomenda a granel e outros encargos adicionais, e XZ ansiosamente à espera que a seiva de Moringa lhe fosse entregue, tentou em vão contactar com GMN, Kaboré, BBP, AC e ao alegado filho d BBP. Todos tinham desligado seus telemóveis.

Mecanismo, Instrumento e Técnica de BC identificados no caso

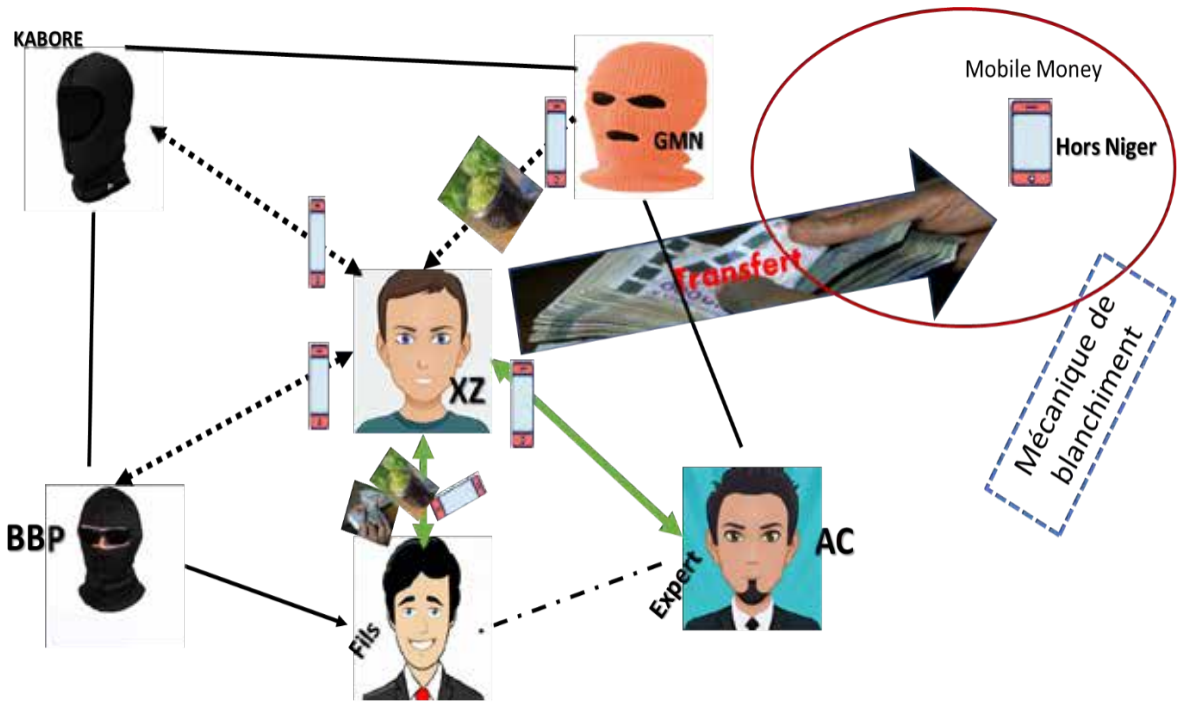
A partir da negociação e da remessa de fundos, XZ conheceu fisicamente apenas duas (02) pessoas: o suposto filho de BBP que lhe entrega a amostra para análise e o perito AC encarregado de analisar a referida amostra. Todas as manobras fraudulentas que tiraram a vontade de XZ de entregar os seus fundos só foram possíveis graças a um método bem conhecido no cibercrime: a engenharia social via TIC.

A infração subjacente de fraude de comunicação eletrónica gerou fundos que foram depositados numa *carteira* de dinheiro móvel e iniciaram um processo de empilhamento (transferência para fora) usando o mesmo aplicativo de dinheiro móvel.

No momento das detenções, os suspeitos estavam na posse de telemóveis, cartões SIM, recibos de transferência de fundos, documentos falsos de identidade utilizados para levantamentos, bem como sacos contendo sementes pretas.

Os suspeitos foram encaminhados para o Ministério Público por fraude através de comunicação eletrónica sem terem sido instruídos pela OPJ com base no crime de branqueamento de capitais.

Fonte: Níger



Caso 9: Fraude nos Serviços de Frete do Comércio Internacional e Fraude de Pagamento Adiantado

Este caso teve início em princípios de 2012, quando o arguido chamou a atenção da UIF por suspeitas de fluxos ilícitos recebidos nas suas contas bancárias. O arguido decidiu esconder-se quando a sua conta foi congelada e mais tarde ressurgiu em 2016 com múltiplas identidades. O arguido utilizou três passaportes diferentes com nomes diferentes para abrir e movimentar sete contas em diferentes agências do Banco "A". O arguido tinha ainda contas em outros quatro bancos, que abriu com recurso a documentos falsos, como passaporte e título de eleitor falsificados. O acusado então apresentou-se para as suas vítimas, fraudulentamente, como um empresário *online* usando os nomes George Hanson e Daniel Brown, que estava nos serviços internacionais de agenciamento de carga em todo o mundo. O esquema está estruturado de tal forma que os seus serviços são recomendados por supostos clientes (seus coconspiradores) de vítimas (potenciais clientes) maioritariamente dos EUA, Reino Unido e outros países como a Austrália que acabam por fazer pagamentos antecipados pelos seus serviços. Ele recebeu das vítimas mais de 20 remessas totalizando 351,000 USD e mais GBP40,000 em suas múltiplas contas.

A investigação apurou que o arguido utilizou parte do produto do crime para adquirir uma casa no Gana. Gastou parte do dinheiro e tinha um saldo de 10,000 libras esterlinas na sua conta, que foi congelada durante a investigação. Foi acusado de branqueamento de capitais, burla com falsos pretextos, evasão fiscal, falsificação de identidade, falsificação de documentos, entre outros. Em tribunal, apesar do arguido ter-se declarado inocente de todas as acusações, o tribunal considerou-o culpado e condenou-o a dois anos de prisão e a uma multa de três mil unidades de pena, ou, à revelia, mais três anos, por falsificação depois da acusação ter provado o seu caso. Acusado de branqueamento de capitais, o arguido foi considerado culpado e condenado a uma pena de dois anos e a uma multa de quatro mil unidades de pena ou, na falta de pagamento, a quatro anos de trabalhos forçados. O tribunal também ordenou o confisco de todos os fundos do arguido e os bens em terrenos, incluindo a casa adquirida, foram confiscados a favor do Estado, além das 10,000 libras esterlinas pendentes na sua conta bancária.

Fonte: Gana

Caso 10: Fraude de Romance / Herança e Fraude de Pagamento Adiantado

Estudo de Caso 1 (Caso de Esquema de Fraude de Romance e Herança)

O acusado foi preso pelo seu envolvimento num grande esquema para fraudar um morador de Nova York, nos Estados Unidos, no valor de 700 mil USD. O arguido (um homem), usando uma identidade feminina falsa (Sra. X), iniciou uma relação amorosa online com a vítima. O acusado contratou os serviços de uma popular atriz pornográfica, Sra. Y, residente nos Estados Unidos, que se apresentou erroneamente como SRA. X para fazer o relacionamento parecer real. A atriz pornográfica convenceu a vítima de uma herança em ouro que ela tinha no Gana e ambas vieram para Gana. No Gana, conheceram um taxista chamado "Z", que acabou por ser o arguido e o mentor. A Sra. X apresentou documentos falsos à vítima mostrando que ela herdara uma mina de ouro de nome Empresa A e queria transferir o mesmo para os nomes conjuntos dela e da vítima. Consequentemente, a vítima transferiu um montante total de 428,865 USD para as contas bancárias de uma empresa que acabou por ser propriedade do arguido e outros 349,993 USD para uma empresa imobiliária, sob a instrução do arguido, como pagamento pelo ouro. Durante a investigação, a empresa imobiliária que recebeu 349,993 USD alegou que os acusados contrataram a empresa para projetar e construir uma mansão para ele numa área nobre de luxo em Acra, Gana. Da mesma empresa fraudulenta, o arguido construiu e mobilou uma mansão de 3 quartos para o pai, tendo também adquirido uma viatura particular - Hyundai Tucson.

O arguido foi acusado de branqueamento de capitais, falsificação de identidade, burla com falsos pretextos, falsificação de documentos e foi constituído arguido perante o Tribunal Superior – Divisão de Crimes Financeiros. Em agosto de 2020, enquanto decorria a acusação, o Tribunal foi notificado da morte do arguido. O Tribunal ordenou o congelamento dos bens dos arguidos e foi nomeado um Administrador-Geral para supervisionar o património do arguido, em conformidade com a Lei da Administração do Património, de 1961, a pedido do EOCO. O pai do arguido intentou uma ação de improcedência do pedido feito contra o arguido, de que uma vez que o pedido inicial foi interposto contra o arguido, que faleceu, o mesmo é incompetente e deve ser julgado improcedente. No entanto, o caso foi avaliado à luz da Secção 50 da Lei da Criminalidade Económica e Organizada, que habilita o Tribunal a confiscar bens contaminados se a pessoa a quem os bens foram apreendidos morrer ou fugir, pelo que o tribunal decidiu a favor do EOCO.

Fonte: Gana

Caso 11: Fraude com o esquema de Romance e Fraude de Pagamento Adiantado

O NFIU recebeu uma comunicação de operação suspeita apresentada por uma entidade sujeita envolvendo várias transações de alto volume num total de de NGN 4,981,206,32. Os fundos foram recebidos por um Sr. X entre 2 de julho e 17 de agosto de 2020, em 10 transações via Western Union Money Transfer. As transações foram enviadas do Canadá pela Sra. Y sem nenhuma justificativa ou evidência de uma relação familiar. As transações de alto volume são um sinal de alerta, assim como o padrão de estratificação das transações para evitar o limite máximo. A localização e a idade do destinatário também levantam suspeitas de um golpe romântico. O caso foi encaminhado para a agência de aplicação da lei competente e está atualmente a ser investigado por Golpe Romântico, fraude com pagamento adiantado e branqueamento de capitais.

Fonte: Nigéria

Caso 12: Golpe do Romance / Falsos Pretextos e Fraude de Adiantamento de Taxas

Este caso foi denunciado à polícia em 2022, em que os suspeitos, que se acredita serem nigerianos e a viverem na Nigéria, abriram várias contas usando nomes falsos e fotos de belas senhoras brancas e, posteriormente, atraíram homens para um relacionamento *online*. No processo, fazem suas vítimas acreditar que precisam preparar um determinado documento chamado "declaração de confiança para relacionamento à distância". Na sua tentativa de obter este documento, as vítimas seriam encaminhadas para um suposto advogado que se acredita fazer parte da associação criminosa que irá extorquir dinheiro das vítimas em nome do fornecimento do tal documento.

A investigação apurou que os referidos suspeitos conseguiram burlar as suas vítimas numa quantia de D587, 700,00 (quinhentos e oitenta e sete mil, setecentos dalasis) (USD 10,494,6) que foi remetida para as contas bancárias na Nigéria.

Que uma carta de correspondência foi enviada à Interpol Nigéria na tentativa de localizar o suspeito e possível recuperação do dinheiro obtido ilegalmente de suas vítimas, mas nenhuma resposta foi recebida até agora.

Fonte: Gâmbia

Caso 13: Tráfico de Seres Humanos, Rapto, Extorsão sexual e Extorsão

Num caso tratado pelo DSC, um líder de uma rede cibercriminosa, aproveitando-se da difícil situação de vida de duas jovens nigerianas, levou-as para o Senegal, sob o pretexto de que conseguiria arranjar-lhes emprego.

Uma vez em Dakar, confiscou-lhes os documentos de viagem, fez-lhes teste de HIV e SIDA e, em seguida, forçou-os a uma forma de escravidão sexual sob pena de morte.

Ele fotografou as meninas nuas e usou as imagens como isco para atrair suas vítimas em suas atividades cibercriminosas.

Ele também os forçaria a dormir com europeus que ele convidava para irem ao Senegal, onde os sequestrava e libertaria depois que seus familiares pagassem um resgate.

O seu modus operandi consistia em contactar a sua presa pelo Messenger, apresentando-se com perfis de raparigas. A partir daí, ele usava os perfis para se comunicar via WhatsApp com as vítimas para tranquilizá-las. Foi com base nestas manobras que conseguiram atrair cinco (05) cidadãos europeus, que foram sequestrados e libertados após o pagamento de resgates.

Esta rede altamente estruturada dispunha de sucursais na sub-região, onde alguns membros do grupo se encarregavam de levantar os fundos das suas atividades que transferiam através de sistemas de transferência electrónica.

A fim de recuperar o dinheiro transferido como resultado da chantagem, o líder da quadrilha cooperou com alguns funcionários da agência de transferência de dinheiro que entregaram os fundos apesar do procedimento normal.

Fonte: Senegal

Caso 14: Fraude, chantagem, extorsão e branqueamento de capitais

Em 2022, MSD, um motorista-aprendiz da cidade de Koundara, na Guiné, que regressava à sua cidade natal, depois de uma longa estadia num país vizinho, decidiu envolver-se em atividades cibercriminosas como meio de sustento. Criou uma conta no Facebook e fingiu ser uma mulher chamada AB, postou várias fotos de uma mulher com estatura física atraente de uma conta do Instagram e enviou convites para vários homens maduros que responderam aos seus pedidos.

Assim, começou entre o MSD agindo sob a identidade de AB e suas vítimas, conversas íntimas durante as quais propuseram a esta última manter relações carnais em modo de chamada de vídeo e conseguiu filmar suas vítimas, a quem ele então chantageou ameaçando-os para pagarem entre 5,000 e 10,000 dólares americanos por mês ou correr o risco de ver suas nudez exposta nas redes sociais.

As vítimas eram geralmente homens respeitáveis, por isso pagaram as quantias solicitadas. Os vários montantes angariados foram utilizados pelo cibercriminoso para montar vários projetos: a compra de um miniautocarro para transportes públicos, um carro de uso pessoal e a construção de um videoclube e de um bar. Estes montantes foram estimados em mais de 50,000 dólares americanos.

Depois de receber várias denúncias, a unidade de cibercrime da direção central da polícia judiciária, sem hesitação, empreendeu investigações digitais que levaram à detenção do suspeito, que reconheceu sem rodeios os factos contra si e pediu clemência às autoridades responsáveis pela aplicação da lei. No final das investigações, o arguido foi encaminhado para o Ministério Público de Kaloum, que solicitou a abertura de um inquérito judicial pelos crimes de burla, chantagem e extorsão, tudo através de um sistema informático e branqueamento de capitais.

Até à data, o processo resultou num julgamento e o infrator condenado a cinco anos de prisão e a uma multa de 500,000,000 GNF pelo Tribunal Criminal de Kaloum e os seus bens confiscados de acordo com as leis LBC/CFT e de Cibersegurança. O MSD está detido na prisão central de Conacri.

Fonte: Guiné

Caso 15: Fraude com contratos comerciais (importação/exportação) e Fraude de pagamento adiantado

Em julho de 2022, um cidadão ucraniano apresentou uma queixa no EOCO alegando que foi burlado em 6,5 milhões USD. O Sr. X, um cidadão nigeriano residente no Gana, foi contratado para fornecer ao Sr. F, um cidadão ucraniano, postes de madeira teca do Gana em 2018. Fotos dos postes de teca supostamente embalados em armazéns alfandegados, além de documentos de embarque, foram enviadas ao ucraniano como prova de que a mercadoria estava prestes a ser enviada. O ucraniano desembolsou os 6,5 milhões USD via transferência bancária como pagamento pelo produto. Posteriormente, o ucraniano nomeou dois advogados ganeses V e K para supervisionar as transações. V e K alegadamente descobriram que a transação era uma farsa, mas levaram o ucraniano a fazer pagamentos. O advogado V confirmou ter recebido honorários legais do ucraniano, bem como 600,000 ceddis do Sr. X. Tanto o Sr. X, V e K foram presos acusados de branqueamento de capitais e conspiração para fraudar e fraude com falsos pretextos. Encontram-se atualmente sob custódia da EOCO.

Fonte: Gana

Caso 16: Fraude, chantagem, extorsão e branqueamento de capitais

Em dezembro de 2022, AOK, um empresário residente no distrito de Sonfonia, na comuna urbana de Ratoma/Conacri, recebeu um telefonema de um desconhecido que lhe disse do outro lado do telefone que ele era um grande adivinho. Assim, o estranho descreveu-o e deu-lhe informações precisas sobre a sua família, as suas atividades, a sua privacidade e depois revelou-lhe que ia correr um grande perigo se não fizesse grandes sacrifícios para evitar o que estava prestes a acontecer-lhe. Os sacrifícios propostos incluíam: 10 bois, 2 camelos, 5 ovelhas a serem sacrificados e uma quantia de 25 milhões de francos (2.500 dólares) a serem usados para comprar outros itens que deveriam ser considerados para o trabalho oculto.

O estranho aconselhou-o a não explicar a situação a mais ninguém, nem mesmo à sua mulher, porque correria o risco de ser afetado pela loucura. Aconselhou-o a agir rapidamente porque o tempo era essencial. Atônito, chateado e assustado com tais declarações inesperadas e temendo por sua vida, o senhor reuniu a quantia de 25 milhões, bem como o valor dos animais mencionados acima, perfazendo um total de 110,000,000 FG (11,000 USD). Ele pediu ao estranho, que é ninguém menos que IKK, para indicar como ele poderia enviar-lhe essa quantia o mais rápido possível.

O suspeito deu-lhe assim 5 números de telefone com contas de dinheiro móvel para os quais pediu- lhe para dividir os depósitos do montante, à razão de 22,000,000 FG por conta. Depois de efetuar o pagamento, o suspeito pediu-lhe para ir buscar água do mar à meia-noite, deitar essa água num frasco ainda sem uso e novo, para adicionar leite de vaca fresco à água e para branquear com a mistura na manhã seguinte, observando o jejum durante todo o processo. Pediu-lhe para ficar afastado durante 3 semanas, após o ritual, sem tocar numa mulher.

Um mês depois de realizar o ritual, AOK recebeu outro telefonema do suspeito que ainda o informava de outro sonho, incluindo os seus filhos, rodeados por uma matilha de cães pretos que ameaçava devorá-los e que o destino tinha de ser rapidamente travado para evitar que as crianças fossem vítimas de feitiçaria. Como na primeira vez, ele indicou animais para sacrificar e uma quantia de 26 milhões (2,600 dólares) a pagar. Assustado com esta nova revelação, AOK recusou-se a cumprir e alegou que já não tem meios para enfrentar a nova exigência do adivinho. O suspeito ao ouvir isso começou a ameaçar AOK, em outros números e, às vezes, através de intermediários.

Preocupado com a situação, AOK decidiu informar a esposa, indo contra o aviso do tal adivinho. A mulher informou o irmão, que é agente de polícia judiciária, que aconselhou o cunhado, a apresentar de imediato queixa na Unidade de Cibercrime da Direção Central da Polícia Judiciária.

Ao receber a denúncia de AOK, a Unidade de Cibercrime da Direção Central da Polícia Judiciária, sem hesitação, iniciou de imediato as investigações, estudando a identificação digital dos utilizadores dos vários números utilizados para os contactos. Assim, foi enviada uma requisição à ARPT com o objetivo de comunicar o histórico de chamadas recebidas e efetuadas dos números suspeitos, bem como a geolocalização dos utilizadores. Os resultados das investigações digitais indicaram que os telefonemas vieram de Labé, especificamente do centro de detenção. Foi enviada uma missão, sob a direção do Ministério Público, para repreender os arguidos que operam a partir deste centro de detenção. Após meio dia de buscas nas várias celas, foram apreendidos 22 telemóveis. Após intensas investigações, os presos finalmente colaboraram e denunciaram seus companheiros de prisão envolvidos no golpe, alguns dos quais já haviam retirado os chips dos telefones.

Quando questionado pelos investigadores, IKK, o principal autor, confrontado com o facto consumado, reconheceu os factos de fraude e extorsão através de um sistema informático de que a AOK era vítima, e denunciou os seus cúmplices que eram ninguém menos que ELMO, que desempenhava o papel de vendedor de gado, ELGA que era responsável por se deslocar aos vários quiosques de dinheiro móvel para levantar as várias quantias. Denunciou ainda FORCE, o guarda prisional que não só facilitou a aquisição de telemóveis, como também serviu de canal para recolher dinheiro em nome do suspeito no exterior da casa de detenção, em troca de subornos. O IKK denunciou ainda dois criadores de gado e um açougueiro que lhe permitiram branquear o produto dos seus atos cibercriminosos.

No final das investigações, o arguido e os seus cúmplices foram encaminhados para o Ministério Público de Labé, que solicitou a abertura de um inquérito judicial pelos crimes de burla, chantagem e extorsão, tudo através de um sistema informático e branqueamento de capitais. Até à data, todos os arguidos foram encaminhados para o tribunal de primeira instância, no Tribunal Criminal de Labé.

Fonte: Guiné

Caso 17: Fraude, falsificação de identidade, fraude de pagamento adiantado e branqueamento de capitais

O EOCO recebeu uma relatório analítico do Centro de Informação Financeira (CIF) em janeiro de 2017 em que o primeiro acusado (A1), um cidadão estrangeiro e titular de passaporte dos EUA recebeu várias remessas totalizando GHS1.551.953,55 (USD309,000) na sua conta num banco em Gana. Descobriu-se que A1 abriu e operou a conta bancária com cartão de identidade falsificado e outros documentos falsificados que enganosamente o identificavam como embaixador da ONU. A1, antes de abrir a sua conta bancária, também tinha recebido várias remessas através de transferências MoneyGram e Western Union.

Quando os fundos da A1 foram detidos, devido à natureza suspeita, para uma investigação mais aprofundada, o segundo arguido (A2), usando documentos falsificados em nome de ministros proeminentes do Gana, apresentou-se como advogado da ONU no Gana, e tentou obter a libertação dos fundos para a A1. A2 alegou que os fundos eram de Singapura e deveriam ser dados à A1 para ajudar a pagar instituições como o Ministério das Finanças e o Banco do Gana por alguns alegados projetos da ONU que estavam a ser executados no Gana. A1 alegou que estava no Gana

para realizar um projeto para refugiados e que era embaixador eleito da ONU para refugiados desde 2015. No entanto, as investigações revelaram que a A1 não era representante da ONU e nunca tinha realizado qualquer projeto para a ONU. As investigações revelaram que essas remessas eram produtos de crimes, cuja origem e finalidade A1 e A2 procuravam dissimular.

O terceiro arguido (A3), então gerente da agência do banco onde A1 abriu a sua conta, violou deliberadamente os procedimentos de abertura de conta e os regulamentos de Conheça Seu Cliente (KYC) para permitir que A1 recebesse e dissimulasse os fundos "sujos". O banco, ao detetar as violações, apresentou uma comunicação de operação suspeita (COS) ao CIF, que também remeteu o caso para EOCO para investigação. A investigação não conseguiu entrevistar os remetentes para confirmar que as remessas eram fraudulentas, e não houve queixas de roubos ou fraudes apresentadas contra os acusados pelos remetentes. Todas as tentativas feitas pela investigação, incluindo o recurso ao auxílio judiciário mútuo, revelaram-se inúteis. Não obstante, os suspeitos foram, por conseguinte, acusados de branqueamento de capitais, falsificação de documentos, falsificação de identidade, fraude mediante falsos pretextos, cumplicidade na falsificação, auxílio e cumplicidade no branqueamento de capitais, em violação das seções 1 e 2 da então Lei de Branqueamento de Capitais, de 2008 (Lei 749), desobediência a uma obrigação contrária à Lei da Imigração, de 2000 (Lei nº 573) e acusações de evasão fiscal contrárias à seção 149 da então Lei das Receitas Internas, 2000 (Lei 592). O processo ainda está em curso.

Fonte: Gana

Caso 18: Fraude de comércio eletrónico, falsificação de identidade e fraude de pagamento adiantado

Em outubro de 2021, a Sra. ANDA de Bafata, entrou em contato com a polícia, sobre um suposto golpe online perpetrado por um suspeito do país vizinho. O suspeito estaria supostamente vendendo cabelos artificiais exibidos na sua página no Facebook com o nome Tafa Cabélo. O suspeito entra imediatamente em contato com as vítimas assim que elas manifestam interesse em comprar o cabelo. O suspeito Tafa disse à Sra. ANDA que o cabelo que ela queria custava 190,000 FCFA (300 USD), mas ela teria de fazer um pagamento adiantado via dinheiro móvel de 50,000 FCFA (95 USD) para fazer o pedido. Como a Sra. ANDA estava interessada, enviou o dinheiro móvel. Sem ter notícias do suspeito durante semanas, ela ligou para perguntar sobre a encomenda, ao que o suspeito respondeu que a sua carga estava prestes a chegar. Depois de algum tempo, o suspeito ligou para ela, pedindo para enviar mais 90,000 FCFA para que ele pudesse despachar sua encomenda na fronteira. Este último pedido suscita a suspeita de Anda, que não revelou ao suspeito, mas alertou a polícia fronteiriça de Bissau. Em acordo com a polícia, ela criou uma história, que envolveu seu irmão NANO, residente em Pefine. NANO ligou então para o suspeito, conforme acordado com ANDA confirmando que entregaria a quantia solicitada na fronteira. Mais tarde, a polícia orientou-os sobre como proceder em termos de comunicação com o suspeito, e procederam à detenção do suspeito junto ao posto de combustível ELTON localizado em Bandim.

Além disso, uma análise ao telemóvel do suspeito revelou que há muito tempo enganava mulheres com a alegada venda de cabelo, através da sua conta de Facebook e consequentemente no Messenger e, para o efeito, criou duas contas nas redes parceiras com os seguintes nomes: FALL TÈRANGA EL TIFRÈ e TAFA CABÉLO, para atrair suas vítimas.

O suspeito foi entregue ao Ministério Público para investigação e acusação.

Fonte: Guiné-Bissau

Caso 19: Fraude de contratos comerciais (importação/exportação) e fraude de pagamento adiantado

Em 2019, o órgão responsável pelo combate ao cibercrime recebeu denúncias sobre determinados indivíduos envolvidos em um caso de golpe usando contratos de exportação. Esta quadrilha organizada de dentro do país e do país vizinho através de telefone entrou em contato com a vítima GSS fingindo tê-lo conhecido e conhecido há muito

tempo. Depois de convencer GSS de que eles tiveram algum tipo de conhecimento no passado e alegando ser médico, propôs um acordo de exportação que tem a ver com o fornecimento de raiz "Artemisia". Em seguida, persuadiram GSS da necessidade de efetuar transferências para cobrir os custos de exportação (compra do produto, armazenamento, transporte, embalagem, formalidades aduaneiras e outros) e conseguiram extorquir-lhe dinheiro de forma fraudulenta. GSS transferiu os fundos que foram levantados eletrónicamente (dinheiro móvel, Western Union, etc.). A investigação levou à detenção de SKS e de outros 47 suspeitos, incluindo um cidadão do país vizinho, identificado como membro ativo da gangue.

O assunto foi remetido ao Procurador Especial do CRIET e depois de considerar o acusado culpado, o tribunal condenou SKS a sete (7) anos de prisão com um milhão de multas FCFA (1,522 USD) e ordenou o reembolso de um milhão setecentos e trinta e seis mil cem FCFA (2.642 USD) a GSS.

Fonte: Benim

Caso 20: Golpe do esquema de Romance / Falsos Pretextos e Fraude de Pagamento Adiantado

Em 2019, a principal agência responsável pelo combate ao cibercrime recebeu informações sobre uma gangue de cibercrime organizado residente em Cocotomey, no distrito de Gbodjè. Após investigação e descoberta da localização dos membros da quadrilha, LCD, KRH e DR foram presos em janeiro de 2020. LCD divulgou e usou o perfil de uma mulher para atrair suas vítimas para o golpe do romance, enquanto KRH usa no seu perfil a foto de uma mulher carente em busca de ajuda financeira. Quanto ao DR, este oferece na internet contratos fictícios para garantir empréstimos. KE, um cúmplice que era responsável por fazer saques de fundos gerados a partir dessas atividades cibercriminosas, também foi preso. O caso foi remetido ao Procurador Especial do CRIET, foram julgados e o Tribunal confirmou o crime de cumplicidade na conta de KE e o crime de fraude através de um sistema informático ou de uma rede de comunicação eletrónica, condenando LCD, KRH e DR a cinco (5) anos de prisão cada e uma multa de dois milhões de FCFA (3,044 USD).

Fonte: Benim

Tipologia 5: Fraude usando o Esquema Ponzi e Branqueamento de Capitais

39. A tipologia aqui apresentada é uma que requer maior e urgente atenção tendo em conta o volume e valor dos fundos envolvidos a partir dos casos aqui apresentados. A tipologia está relacionada com ativos virtuais/criptomoedas ou investimentos *online*. Uma combinação de ganância e conhecimento limitado do empreendimento comercial proposto são os fatores motivadores para a maioria das vítimas vulneráveis que foram vítimas dos esquemas usados por esses criminosos. Além disso, o modus operandum aqui utilizado foi possibilitado devido ao quadro regulamentar e de execução/repressvio inadequados nos Estados membros.

Caso 1: Fraude usando o Esquema Ponzi com Ativos Virtuais

A empresa "A" foi constituída em Acra em outubro de 2017 com os seguintes objetivos, que incluem desenvolvimento imobiliário, serviços de transporte, comércio eletrónico, comércio eletrónico, serviços de tecnologia *blockchain*, transferências de dinheiro móvel, construção de estradas, importação de aparelhos de energia solar, serviços de petróleo e gás. Logo após a incorporação, a empresa declarou falsamente ao público ganês que estava licenciada para exercer a atividade de recebimento de depósitos pelo Banco de Gana, quando, na verdade, não estava autorizada a fazê-lo. Os golpistas prometiam às vítimas um retorno mensal de 27% sobre o investimento. A empresa conseguiu receber GHS43.2M (aproximadamente USD9,6M) de pessoas desavisadas. O montante recebido foi dissipado deixando um saldo de GHS3,7M (USD820K) que foi congelado pelo tribunal. Os acusados durante a investigação admitiram que a sua empresa não estava licenciada pelo Banco do Ghana and nem a Comissão de Valores Mobiliários e Câmbio (SEC) para se envolver em tais negócios. Eles também alegaram que estavam a negociar comercialmente criptomoe-

das on-line mas que havia colapsado. Esta alegação não pôde ser mais explorada para poder ser rejaitada ou confirmação pela investigação porque os investigadores não tinham a perícia técnica necessária para averiguar a veracidade das alegações feitas pelos acusados. A investigação, no entanto, estabeleceu que a empresa estava apenas a usar o comércio de criptomoedas como uma cobertura para obter depósitos do público. Em resultado disso, os arguidos foram acusados e estão a ser processados por operar um negócio de recebimento de depósitos sem licença, fraude sob falsos pretextos e evasão fiscal. Nenhuma acusação em relação ao comércio ilegal de Bitcoin foi apresentada porque a investigação não tinha a perícia técnica para explorar se o acusado estava envolvido no negócio de criptomoedas, e o destino dos fundos. O Gabinete de Crimes Económicos e Organizados (EOCO) iniciou a investigação com base em petições e queixas recebidas de algumas vítimas do esquema fraudulento.

Fonte: Gana

Caso 2: Fraude usando Esquema Ponzi com Ativos Virtuais

Em fevereiro de 2020, o suspeito entrou no país por estrada usando rota não autorizada e estava na posse de 10.000 dólares, que não declarou como manda a lei e regulamento. O suspeito registou uma Empresa Individual em Bissau denominada CHAVE DE SUCESSO, junto do Centro de Formalização de Empresas do Ministério da Economia. A Empresa Chave do Sucesso iniciou suas operações financeiras em março de 2020, recebendo depósitos de pessoas físicas com 20% de juros semanalmente. O suspeito criou um cadastro e treinou sua equipe de marketing que mobiliza clientes para investir seu dinheiro na empresa com a possibilidade de ganhar 20% de lucro semanalmente.

Os profissionais de marketing estavam ganhando 60.000 FCFA (100 USD) por seu serviço e uma comissão adicional de 3% sobre o valor depositado por cada cliente que trazem para a empresa. Para convencer as vítimas, o suspeito apresentou os dados da sua conta bancária domiciliada num banco da capital Bissau, na qual alegava estar a fazer transferências para comprar moeda virtual. Informou as vítimas de que a sua empresa tinha uma conta na plataforma binimo.com que, devido à fraca facilidade de internet em Bissau, não tem estado ativa na plataforma.

Embora a empresa suspeita esteja registada em Bissau, a empresa não estava registada nem licenciada para se dedicar à aceitação de depósitos. A investigação revelou que o suspeito pagou inicialmente 5,7 milhões de FCFA (95.000 dólares) do depósito de 70,8 milhões que recebeu no mês de maio de 2020. Em julho de 2020, o suspeito tinha pago a 3174 investidores o dinheiro com os respetivos juros no montante de 917.471.400 FCFA (1,53 milhões USD) e ainda devia a 1409 investidores a quantia de 532.249.200 FCFA (900.000 USD), incluindo juros acumulados de 20% no valor de 443.341.000 FCFA (740.000 USD).

O suspeito foi detido pela PJ e detido na sua empresa 85.361.500 FCFA (142.000 USD). Foi acusado de fraude, incluindo fraude fiscal e branqueamento de capitais. Ele foi condenado a uma pena de prisão de 10 anos e a reembolsar suas vítimas com a soma de 532.249.200 FCFA (900.000 USD). Além do reembolso, ele deve compensar suas vítimas com a quantia de 75.000.000 FCFA (125.000USD).

Fonte: Guiné-Bissau

Caso 3: Fraude no Esquema Ponzi de Ativos Virtuais

Um jovem com um pouco de conhecimento das TIC elaborou um plano para operar um esquema Ponzi. Ele descaradamente publicou anúncios e jingles nas redes sociais e rádios comunitárias em áreas rurais dizendo que está operando um negócio de criptomoedas. Seus jingles e anúncios prometiam 22% de juros sobre o capital por 2 semanas e 44% todos os meses. Em menos de dois meses, acumulou cerca de 5 mil milhões de dólares (294.724,65 USD).

A UIF utilizou os seus poderes administrativos e restringiu os fundos. O Banco da Serra Leoa foi imediatamente notificado, tendo sido enviado um relatório de informações ao Diretor dos Serviços Criminais da Polícia da Serra Leoa. Entre os depositantes deste esquema estavam políticos locais, policiais, professores, agricultores rurais, estudantes etc.

As investigações revelaram que ele tinha uma carteira de criptomoedas que tinha apenas 800 USD. As investigações revelaram ainda que ele não estava envolvido em negócios de criptomoedas, mas em um esquema Ponzi. O Supremo Tribunal foi chamado a pronunciar-se sobre esta questão.

Fonte: Serra Leoa

Caso 4: Fraude do Esquema Ponzi Online

VH, um jovem empresário, tinha o hábito fazer saques frequentes usando o serviço de dinheiro móvel. Ele faz levantamentos de grandes somas diariamente usando vários pontos de dinheiro móvel. Para realizar as suas transações, ele tem vários cartões SIM. Assim que um dos cartões SIM atinge o seu limite de retirada autorizado, ele o substituiu por um novo para continuar as operações. Essas atividades frequentes despertaram a desconfiança da operadora, que inicialmente pensou que havia um mau funcionamento na sua plataforma. Para confirmar a suspeita, a operadora apresentou queixa ao principal organismo responsável pelo combate ao cibercrime (PLCC). A PLCC, apoiada pelo Laboratório Forense Digital, iniciou investigações que levaram à detenção de VH. Quando levado ao local e após interrogatório, disse que pertencia a uma rede e que tinha sido recrutado para fazer levantamentos com cartões SIM que lhe foram disponibilizados. Os fundos retirados, segundo ele, vieram de um site de investimentos online na bolsa de valores chamado ANTP, cujo link é: https://www.antp.io. Este site convida os indivíduos a investir um montante à sua escolha para um maior retorno sobre o investimento. O dinheiro investido deve aumentar de acordo com o número de tarefas diárias a serem feitas no site. Os membros não tinham ideia do engano. De fato, eles notaram o aumento de seu saldo na plataforma, como prometido. No entanto, alguns dias depois, foram bloqueados e quase não receberam a sua parte devida. Com exceção de alguns que receberam dinheiro nas suas contas de negócio móveis, como forma de levá-los a investir mais e atrair o número máximo de pessoas. Como resultado da busca e apreensão, a PLCC prendeu 12 membros da rede. São eles ZQ, XC, KY, MK, TBF, SL, SAM, MT, ME, MA, KKY, MM. Tinham na sua posse centenas de telefones, 08 laptops e a soma de 46,553.000 francos CFA (75.000 USD).

A perda provisória foi estimada em mais de 1,000,000,000 francos CFA (1,6 milhões de dólares). Várias transações foram realizadas e os fundos depositados em uma conta bitcoin para contornar os mecanismos. (O caso ainda estava em andamento no momento deste relato;

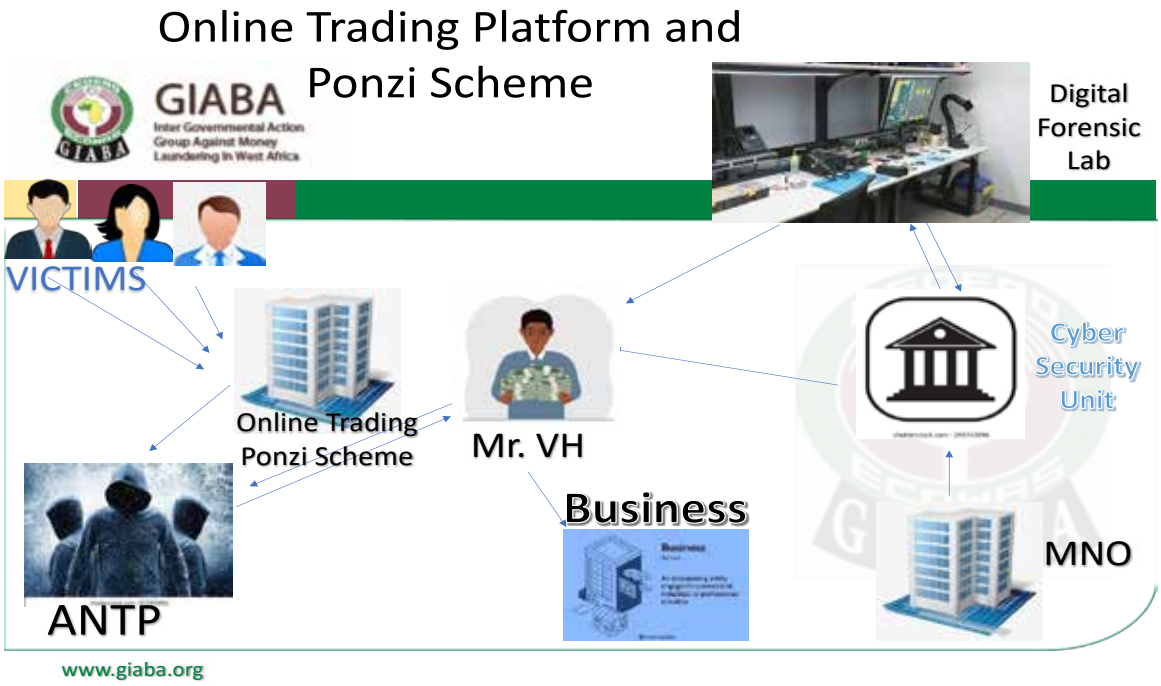
Fonte: Cote d'Ivoire

Métodos e técnicas

- Criação de sites de esquema Ponzi com recursos a plafatformas de comércio eletrónico e de investimento.
- Ativar *Pop-up*s de site nas páginas de rede social de potenciais vítimas.
- Fazer pagamento parcial inicial às vítimas/investidores para atraí-los a investirem mais e fazer com que outros confiem no processo.
- Aumento fictícios da Taxa de Juros das vítimas/investidores para atraí-los a investir mais.

Sinais de alerta e Indicadores

- Oportunidades de investimento não presenciais com *start-ups* online.
- Oferta de negócio irrealista – Super lucro devido à Taxa de Juros muito alta.



Caso 5: Fraude do esquema Ponzi através de investimentos com dinheiro móvel

Em 2022, um caso de investimento falso foi denunciado ao Esquadrão de Fraude da Força Policial da Gâmbia por 146 vítimas. O tal investimento designado Qubid foi introduzido na Gâmbia por um nome fictício Marcus Gabel que se acredita estar na Nigéria. Ele recrutou agentes na Gâmbia para realizar a suposta forma de negócio a natureza do negócio em que o agente incentiva as pessoas a investirem com eles através de dinheiro móvel e depósito bancário e receber o seu capital e juros de 20% depois de sete dias.

O primeiro grupo de pessoas que investiu recebeu suas várias participações de capital, que incentivou muitas pessoas a investirem no negócio. 146 pessoas investiram um montante total de D24.526.993 (437,982 USD) foi investido no negócio. Parte do dinheiro investido foi usado para pagar capital e juros dos investidores cujo investimento havia vencido. Que um dos agentes enviou a quantia de D2, 834.000 (50,607 USD) em Bitcoins e D551.125 (9.,41) para Marcus que estava na Nigéria. Esse dinheiro devia constituir fundos do investimento.

A investigação revelou que a referida empresa nunca esteve registada na Gâmbia e que quem iniciou o negócio estava na Nigéria e estava a gerir/controlar o negócio através de um grupo de WhatsApp. Os 4 agentes foram acusados de branqueamento de capitais, obtenção de dinheiro mediante falso pretexto e realização de negócios bancários na Gâmbia sem licença e estão atualmente a ser julgados no Tribunal Superior da Gâmbia.

Fonte: Gâmbia

Caso 6: Fraude através de investimento no comércio eletrónico

Durante o ano de 2019, a Brigada Central de Luta contra o Cibercrime (BCLCC) recebeu várias vítimas que queriam apresentar queixa contra a empresa Chymall por fraude e quebra de confiança, tendo causado prejuízos de mais de mil milhões de francos CFA.

Da audição do responsável da empresa, verifica-se que a empresa aderiu a uma plataforma de comércio *online* chamada SAIRUI. Com a evolução da sua atividade, foram promovidos a um centro mediante o pagamento de uma quantia de dez mil (10,000) dólares. A sua posição como centro transformou-os em intermediários através dos quais outras pessoas poderiam aderir a esta plataforma, receber os produtos e os seus possíveis bónus. Em junho de 2020, na sequência da mudança de nome da empresa que passou a chamar-se Chymall, foi criada uma representação no

Burkina Faso. Começaram então a inscrever outras pessoas que queriam aderir à plataforma, sob o patrocínio dos líderes. As coisas correram normalmente durante algum tempo e as pessoas que acederam à plataforma através do seu centro começaram a receber os seus bónus de acordo com as taxas definidas pela Chymall. No entanto, em novembro de 2020, começaram a enfrentar desafios de pagamento e anomalias que não os permitia cumprir as regras pré-estabelecidas. Além disso, todas as contas na plataforma sofreram alteração.

Uma investigação mais aprofundada revelou que a empresa-mãe estava sediada na China, com representação no Gana. Até à data, temos mais de mil (1000) vítimas com danos que ascendem a mais de mil milhões de francos CFA (1,6 milhões de dólares) que não foram localizados.

Fonte: Burkina Faso

Caso 7: Fraude no esquema de empréstimos eletrónicos / não presencial

O Sr. AS se envolve em crimes cibernéticos postando mensagens de empréstimo on-line usando identidades falsas, a fim de defraudar suas vítimas. A investigação levou à detenção de AS, residente em Abomey-calavi, no distrito de Bidossessi, em setembro de 2019. Após a sua detenção, AS foi encontrado com documentos falsos relativos a contratos de empréstimo, ordens de transferência, certificados de garantia de seguro, cópias de transferência de dinheiro encontrados no seu telefone e computador portátil na sua posse. Ele alegou ter usado os recursos que extorquiu das vítimas para pagar uma viatura, abrir uma loja de roupas e fazer outros investimentos. Ordenou às suas vítimas que pagassem em adiantado os custos de garantia dos empréstimos para as contas bancárias pertencentes aos seus cúmplices que, por sua vez, faziam os levantamentos. O caso foi encaminhado ao Procurador Especial do CRIET em setembro de 2022. AS foi julgado e condenado a cinco (5) anos de prisão e uma multa de quinhentos (761 USD). Todos os bens relacionados com o caso foram confiscados.

Fonte: Benim

Tipologia 6: Fraude e branqueamento de capitais associado ao dinheiro móvel

40. A segunda tipologia mais popular depois do esquema de fraude usando o pagamento adiantado na África Ocidental, é a fraude relacionada com dinheiros móveis. Existe uma linha ténue entre a fraude através de pagamento adiantado e outras fraudes relacionadas com dinheiro móvel. Na verdade, quase todas as fraudes de pagamento adiantado são facilitadas pelo telefone celular e, na maioria dos pagamentos pequenos e médios, usam a plataforma de dinheiro móvel para receber os pagamentos adiantados exigidos ou solicitadas. Alguns dos casos apresentados no âmbito da fraude através do pagamento adiantado podem igualmente ser adequados para serem apresentados como fraude relacionada com dinheiro móvel.

Caso 1: Falsos pretextos, Falsificação de identidade, Falsificação e Fraude com dinheiro móvel

Uma agência da linha de atendimento ao cliente de um banco recebeu uma chamada supostamente da sede do banco. O interlocutor identificou-se como membro do comité executivo (EXCO Member) usando o nome de Chef Responsável das Operacões (COO). Após uma breve conversa elefónica com o Serviço de Apoio ao Cliente, pediu para falar com o caixa que gere as operaçõe Dinheiro Móvel na agência. A ligação foi transferida para o caixa, onde ele indicou ao caixa que queria guiá-lo através deo procedimento de como realizar reversão do dinheiro móvel na plataforma Momo. Em seguida, solicitou ao caixa que introduzisse o PIN do MoMo e, ao introduzir o PIN, o suspeito deu uma série de instruções que o caixa obedeceu. Imediatamente após o suspeito pausar o telefone, o caixa notou que uma quantia total de GHS37.000 (USD6,491) foi transferida fraudulentamente da carteira do Banco para a carteira de um indivíduo, que foi imediatamente retirada.

O caso foi denunciado à polícia que, com a ajuda da MTN Gana, rastreiou o suspeito, um homem de 30 anos, até ao seu esconderijo numa cidade distante e foi detido em março de 2021. Durante as investigações, apurou-se que o cartão de identificação utilizado pelo suspeito para registar o seu cartão SIM era falsificado. O suspeito foi acusado de falsificação de identidade, fazer-se passar por outrém, burla com falsos pretextos e branqueamento de capitais. A acusação ainda está em curso no tribunal do circuito.

Fonte: Gana

Caso 2: Falsos pretextos, burla de falsa identidade, Falsificação e Fraude usando dinheiro móvel

Um suspeito de Sr. ABD foi preso em julho de 2021, por suspeita de suposto golpe através das redes sociais. O suspeito e outros cúmplices usavam o Facebook e o Messenger com um nome de perfil falso (SOIOIO MELA) e ardilosamente enganavam as vítimas, para extorquir dinheiro. Além do Messenger do Facebook, ele também usa números de móveis registados em nomes de outras pessoas para se comunicar com as suas vítimas. As investigações preliminares levaram a polícia a dois indivíduos que tiveram contacto visual com o suspeito, uma vez que este lhes tinha pedido para usarem os seus números de telemóvel, para receberem o dinheiro que lhe era transferido. Esses indivíduos confirmaram que o reconheceriam se o encontrassem. A investigação conciliou as informações acima com a divulgação feita pelo Sr. BILL, mais conhecido como SOIOIO, quando acompanhou uma das vítimas para apresentar queixa à Polícia. O Sr. BILL confirmou à investigação que o suspeito é um indivíduo vulgarmente conhecido como SACA, que, em conluio com a sua sobrinha de nome SC, tinha utilizado o seu telemóvel, que a sobrinha tinha roubado da sua residência em Bula, com o qual tinham cometido atos semelhantes e pondo em causa a sua reputação, uma vez que pediam dinheiro em seu nome, além de enviar mensagens de amor aos amigos e conhecidos, colocando em descrédito a relação matrimonial de algumas das pessoas visadas. Ele conseguiu, no entanto, recuperar o telemóvel com a intervenção da Polícia Judiciária.

O suspeito estava sob custódia do Ministério Público, pronto para ser julgado na Secção Criminal do Tribunal Regional de Bissau, enquanto aguardava-se a perícia do telemóvel (Infinix Smart Dual Camera) que lhe fora apreendido.

Fonte: Guiné-Bissau

Caso 3: Falsos pretextos, burla de falsa identidade e Fraude com Agente de dinheiro móvel

Em fevereiro de 2018, um Tribunal Distrital de Oda, na Região Leste do Gana, prendeu duas pessoas de 28 e 29 anos, respetivamente, por defraudarem um agente de dinheiro móvel. De acordo com a Polícia, os suspeitos ligaram para o dinheiro móvel por telefone e fingiram que eram oficiais da MTN Ghana Ltd ligando para educar o agente sobre suas transações de dinheiro móvel. No entanto, durante o processo, o agente de dinheiro móvel observou que sua conta foi debitada com GHS2000. O agente denunciou o incidente à polícia, que entrou em contato com a MTN e mandou rastrear e prender os suspeitos. Um dos suspeitos alegou ser especialista em Tecnologias de Informação e Comunicação (TIC) e o outro desempregado. Os dois suspeitos foram processados e presos.

Fonte: Gana

Caso 4: Uso abusivo de informação privilegiada, pirataria usando esquema complexo de engenharia e fraude com dinheiro móvel

O Banco X no Gana tinha apresentado uma petição ao EOCO para levantamentos não autorizados feitos a partir de várias contas dos seus clientes através das plataformas de *mobile banking* e *internet banking* do banco. Os saques fraudulentos foram feitos quando os clientes estavam em processo de registo/aceitação no banco eletrónico. Antes da petição do banco X, dois outros bancos, Y e Z, também tinham feito queixas semelhantes sobre levantamentos não autorizados de alguns dos seus clientes através da aplicação *Mobile Banking* e quatro suspeitos foram detidos pelo EOCO. A investigação constatou que os piratas informáticos estavam a executar esquemas complexos de engenharia social direcionados a pessoas desavisadas para obter credenciais de *login* relevantes para os portais bancários eletrónicos. Alguns dos suspeitos tinham obtido dados de clientes (incluindo número de conta, nome da conta, saldo da conta, data de nascimento, morada e números de telefone) dos seus coconspiradores em alguns dos bancos. Munidos

dessas informações, ligavam para os clientes com números clonados que parecem emanar das ligações dos bancos e enganavam as vítimas para que fornecessem seus dados. Uma vez obtidas essas credenciais, os fundos eram distribuídos e branqueados através de um esquema elaborado que incluía o uso de várias contas de dinheiro móvel e contas bancárias de agentes de terceiros. Em alguns casos, poucos momentos após os levantamentos não autorizados, os fundos eram imediatamente levantados dos comerciantes de dinheiro móvel. A investigação ainda está em curso.

Fonte: Gana

Caso 5: Uso abusivo de informação, Falsificação de Identidade e Fraude usando Dinheiro Móvel

Em abril de 2022, o EOCO deteve um funcionário do banco e um funcionário de uma importante rede de telecomunicações que alegadamente estavam coniventes com cerca de quatro pessoas para defraudar alguns clientes bancários através da fraude com uso de troca de cartõesSIM. Os suspeitos contrataram o funcionário do banco para lhes fornecer os dados da conta bancária e números de telefone das suas vítimas com elevados saldos nas contas para ajudá-las a levantar fundos dessas contas, enquanto o pessoal da empresa de telecomunicações foi contactado para clonar os números de telefone das vítimas para a operação. Os funcionários do banco foram coniventes com os arguidos ao fornecerem os dados solicitados e conseguiram clonar números de telefone de cerca de três clientes com a intenção de roubar 850,000 Ceddis do Gana; 680,000 Ceddis do Gana e 50.000 Ceddis do Gana (um total de 216,000 USD), respectivamente, dos clientes. Os arguidos criaram uma aplicação móvel com os SIM clonados para levantar os fundos das contas bancárias dos clientes. Entretanto, o funcionário do banco notificou o Banco sobre o lote e o problema foi comunicado ao EOCO. Os arguidos foram detidos quando tentavam levantar os fundos do Banco. Foram acusados de nove crimes de conspiração para roubar, tentativa de roubo e participação em grupo criminoso organizado. O caso está a ser julgado.

Fonte: Gana

Caso 6: Burla de falsa identidade, dinheiro móvel e fraude com cartões SIM

O Sr. O, um jovem licenciado, criou a sua própria empresa, vendendo cartões SIM, a fim de adquirir independência financeira. Seu negócio estava a ir bem até um dia em que foi abordado por KDU que pediu para comprar 5 cartões Sim. A ideia era usá-los para abrir cinco agências de transferência móvel. O Sr. O ativou os cartões SIM e, como habitualmente, o cliente ficou satisfeito. Ao prosseguir a sua atividade, o Sr. O ficou a saber que os cartões Sim que vendeu a KDU eram utilizados em transações fraudulentas. Ficou surpreendido porque KDU lhe tinha dito que os cartões eram para os cinco caixas nas agências que estava prestes a abrir. KDU tinha fornecido ao Sr. O cinco diferentes documentos de identificação para a ativação dos cartões SIM. Ele ficou preocupado porque também ouviu rumores de que circula um golpe usando carteiras eletrónicas. Além disso, semanas depois, ele foi convocado pela polícia de crimes cibernéticos sobrea um caso semelhante. De facto, a Plataforma de Luta contra o Cibercrime (PLCC) está atualmente sobrecarregada com queixas relacionadas com este tipo de crime. Entre as queixas, há três de vítimas LLF, CNS e MYL que afirmam ter sido contactadas por telefone por desconhecidos, alegando terem feito depósitos por engano para seus números. Para verificar a eficácia das alegadas transações, as vítimas esvaziaram as suas carteiras fazendo depósitos para um número desconhecido. Cada um deles apresentou uma queixa junto da PLCC para resolver o caso.

A investigação da PLCC, apoiada tecnicamente pelo Laboratório Forense Digital, levou à descoberta de que o número que recebia as transferências pertencia a KDU. O suspeito foi detido e estava na posse de 27 cartões SIM. Durante o interrogatório, KDU admitiu ter enganado várias pessoas nas suas contas de telemóvel com os *chips* comprados do Sr. O. A análise do Laboratório Forense aos 27 cartões SIM também revelou que eles foram usados para outras transações fraudulentas. Estes números foram alvo de 136 queixas e efetuaram 308 depósitos fraudulentos no valor de 12,786,202 francos CFA (19,520 euros).

Por fim, KDU foi levado ao Ministério Público de Abidjan, onde poderá ser processado por fraude e cumplicidade em fraude de transações. (O caso ainda estava em andamento aquando deste relato)

Fonte: Cote d'Ivoire

Caso 7: Uso abusivo de informação privilegiada e fraude com agente de dinheiro móvel

Em janeiro de 2022, a Brigada Central de Combate ao Cibercrime foi contactada pelo gerente da empresa C2EGF--BF que apresentou queixa contra um dos seus representantes de venda por falsificação e uso de documentos falsos, quebra de confiança e branqueamento de capitais, causando um prejuízo de mais de trinta e sete milhões de francos CFA (60,000 USD).

Da investigação resulta que o respondente tinha sido recrutado pela empresa C2EGF-BF como representante comercial. A empresa é um distribuidor de Dinheiro Móvel. O trabalho do acusado era recrutar, treinar e auxiliar agentes dos pontos de venda da empresa. Este aproveitou a sua posição comercial para instalar uma senhora e esta telefonou ao nível da empresa para pedir material. Os recibos que justificavam os reembolsos passavam por esta última.

Investigações posteriores levaram à prisão do suspeito. Uma vez que a loja pediu um fornecimentos, um reembolso, este último tinha recibos antigos que tinha digitalizado. Ele usava um recibo antigo, mudava a data, tirava uma foto e enviava para a empresa via WhatsApp como mensagem instantânea. Assim que a mensagem é lida, ela é imediatamente apagada. O respondente usou o dinheiro do seu pacote para criar várias outras lojas de dinheiro Orange em nome dos seus pais e suas namoradas. (O caso ainda estava em andamento no momento deste relato)

Fonte: Burkina Faso

Caso 8: Fraude com Cartão SIM e Roubo de Identidade usando SIM Pré-Ativado de Registos de Eleitores Abandonados

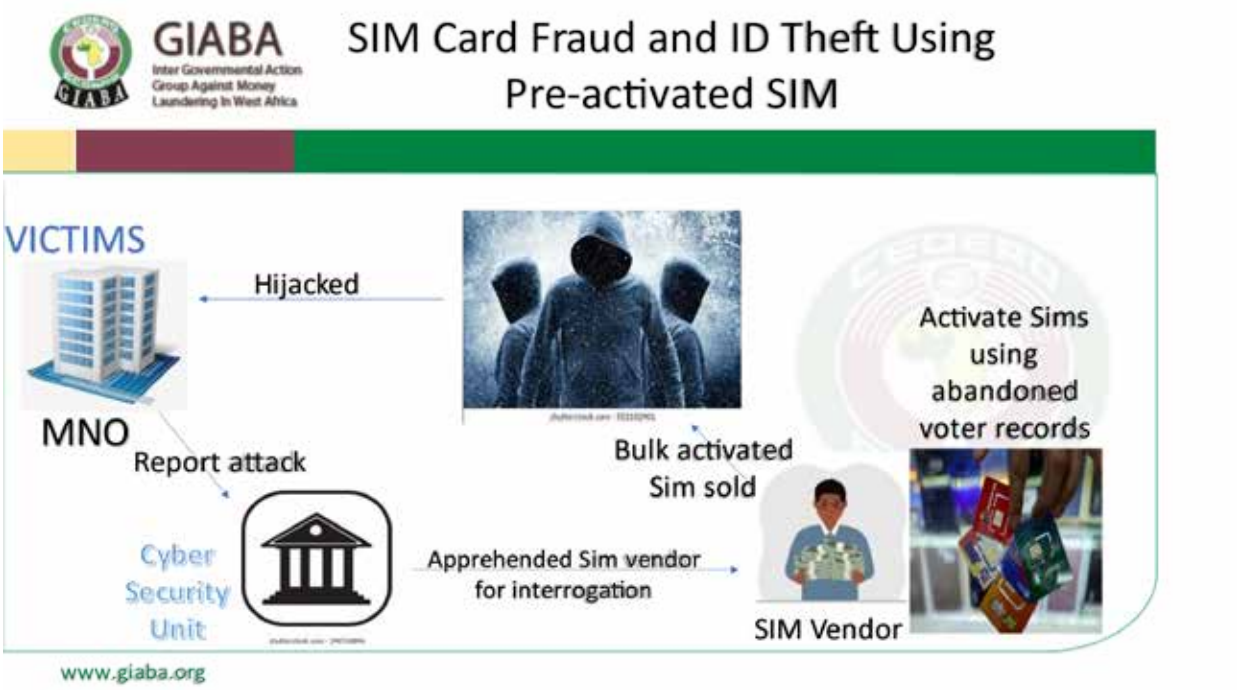
O sistema de rede informática de uma empresa foi pirateado. O *hacker* explorou falhas na segurança da rede e nos aplicativos da empresa para extrair dinheiro do sistema de moeda eletrónica. Na verdade, um *chip* de teste para novos serviços foi criado num departamento sem medidas de seguimento em caso de incidente para determinar as responsabilidades.

O *chip* foi usado para colocar dinheiro em mais de 100 contas de moeda eletrónica. O rastreio do dinheiro é dificultado pelo facto de a identificação e venda dos *chips* não serem muito bem supervisionadas. Assim, o dinheiro deste ataque foi retirado de várias lojas em várias cidades, nomeadamente Dakar e Thiès. Os detalhes das operações sugerem o uso de um meio de transporte para retirar o dinheiro de todas as lojas no eixo Dakar-Thies.

Uma investigação foi aberta após uma denúncia da empresa alvo do ataque. Observou-se que *chips* diferentes tinham sido ativados de antemão sem ser possível estabelecer a identidade dos verdadeiros donos. Esses mesmos *chips* foram mais tarde usados para abrir contas em moeda eletrónica.

As investigações dentro da estrutura não conseguiram determinar a origem da conexão que realizou essas operações fraudulentas. Além disso, não foi estabelecido qualquer sistema de validação de operações ou de vigilância de operações importantes. A investigação foi, assim, direcionada para o rasteio dos chips, a fim de determinar a identidade dos verdadeiros donos e poder identificar o destinatário final das operações. Assim, o vendedor que procedeu à ativação dos diferentes *chips* foi interrogado. Não podendo fornecer a identidade dos compradores, foi realizada uma busca em sua casa. Descobriu-se, assim, que ele próprio tinha procedido à ativação dos diferentes *chips* com base nos dados pessoais constantes do processo eleitoral. Na verdade, após cada eleição, os arquivos eram recuperados e vendidos no mercado. Isso constitui uma falha enorme na aplicação da medida que exige que os operadores telefónicos identifiquem os seus clientes.

Fonte: Senegal



Métodos e técnicas

- Utilização de identidades falsas para se fazerem passar por indivíduos/entidades
- Os burlões fazem-se passar por agentes do serviço de apoio ao cliente e pedem aos utilizadores que partilhem PINs, OTPs (One-Time Passwords) ou detalhes da conta, alegando que estão a ajudar o cliente a "resolver um problema".
- Utilização de números de telemóvel registados em nome de outras pessoas
- Utilização de esquemas complexos de engenharia social para obter credenciais de acesso à plataforma eletrónica de indivíduos/entidades

Sinais de alerta e Indicadores

- Uma conta de dinheiro móvel recebe ou envia repentinamente grandes somas de dinheiro, sem ter em conta a atividade anterior
- Várias transacções de elevado valor num curto período de tempo
- Os fundos são imediatamente levantados ou transferidos para várias contas poucos minutos após a receção
- Série de transferências de fundos de uma carteira ou conta para várias contas ou carteiras em intervalos curtos

Tipologia 7: Casos de Financiamento do Terrorismo facilitados pelo Ciberespaço

41. Como o financiamento do terrorismo continua a ser um fenómeno complexo com o qual a região ainda se debate, nomeadamente compreender o modus operandum que, em grande medida, se crê estar a ocorrer no setor informal e talvez a utilizar o ciberespaço, incluindo a *dark web*, foram apresentados 3 casos que se qualificam como casos de financiamento do terrorismo facilitados pelo ciberespaço.

Caso 1: Financiamento do terrorismo com base no comércio

Um cidadão canadiano de origem somali residente em Dakar tinha criado uma empresa imobiliária no Senegal. A empresa, em conjunto com um senegalês, tinha aberto uma conta num banco em Dakar. Algum tempo depois, a conta recebeu uma transferência de aproximadamente cento e seis mil (106,000) dólares americanos de um cidadão somali residente nos Estados Unidos. A transferência foi executada por uma instituição financeira com sede em Dubai. Suspeit-

ando desta operação, devido à identidade mal documentada do novo cliente e o destino dos fundos, o banco senegalês apresentou uma comunicação de operação suspeita à UIF. A investigação revelou que a empresa não tinha estatuto jurídico no Senegal e que tinha sido criada especificamente para efeitos de branqueamento de fundos ilícitos através da venda de mercadorias importadas. Além disso, os indivíduos envolvidos estavam em contacto com grupos extremistas envolvidos em atividades terroristas na África Oriental, América e África Ocidental. Outras empresas foram criadas, em associação com senegaleses, para importar bens usados, alguns dos quais eram vendidos em Dakar e os restantes exportados para outro país para revenda. O produto destas várias operações comerciais era subsequentemente enviado para vários grupos terroristas através de vários canais. (O caso ainda estava em andamento aquando deste relato)

Fonte: Senegal

Caso 2: Suspeita de angariação de fundos para o financiamento do terrorismo

Em 2015, o Banco XPTO apresentou uma COS relativa a um indivíduo identificado como XMAN, um turco por nacionalidade, residente na cidade da Praia, e um professor independente. Suas transações financeiras incluem fazer saques e transferências em moeda estrangeira para o exterior; ele também recebe fundos especificamente da Turquia. Verificou-se que os pagamentos eram compensados pelo titular do visto em montantes iguais aos créditos depositados em dinheiro no mesmo dia ou no dia seguinte. As operações de compra de moeda estrangeira por um valor consideravelmente elevado sem justificação, considerando que o cliente é um professor liberal como havia declarado ao Banco XPTO.

A movimentação da conta é caracterizada por muitos pequenos montantes de crédito e um pequeno número de débitos de alto valor. A justificação dada por XMAN quanto à finalidade dos fundos é que se destinam a fins religiosos, não se coaduna com os pagamentos reais efetuados por serviços de comunicação, alojamento e viagens frequentes. A ausência de qualquer relação razoável entre a XMAN e a empresa PPP, cujo objeto é a venda de equipamento informático.

Após análise da COS do Banco XPTO, verificou-se que o Sr. XMAN possui duas contas distintas (em moeda nacional e estrangeira), no banco em questão, abertas em setembro e dezembro de 2012, respetivamente. Para a conta aberta em dezembro de 2012, recebeu transferências do banco turco KATILIM BAKAST A. S., no valor total de 5,669,379$00 CV Escudos (51,416 euros), em (04) quatro movimentos dando como razão para as transferências o facto delas se destinarem a efetuar o pagamento de Qurban (sacrifício de animais) e para organizações de orfanatos. Os valores recebidos através das transferências acima indicadas, entre janeiro e maio de 2014, foram utilizados pelo Sr. XMAN para efetuar pagamentos com cheques bancários do XPTO para subsistência e viagens, e não para fins religiosos e de caridade como indicado nas transferências. Os pagamentos foram feitos à empresa PPP que vende equipamentos e QQQ que importa vários produtos alimentares, bem como pagamento a uma agência de viagens.

Entre 2013 e 2014, o Sr. XMAN realizou várias viagens, incluindo 9 (nove) entre PRAIA/DAKAR, 4 (quatro) entre PRAIA/MARROCOS, 5 (cinco) entre PRAIA/PORTUGAL e 1 (uma) PRAIA/BISSAU. O caso em questão ainda está sob investigação.

Fonte: Cabo Verde

Caso 3: Financiamento do terrorismo através de métodos de transferências informais (HAWALA)

Em 2022, os serviços de segurança do Estado colocaram à disposição dos serviços de investigação o Sr. DA, um motociclista e traficante, suspeito de ser colaborador de um grupo terrorista armado liderado por IL. IL é um criminoso procurado, citado em vários casos de extorsão, saques e violência grave contra civis no Níger, incluindo o seu envolvimento em atividades terroristas em Liptako Gourma. IL, de acordo com fontes de informação, lidera um Grupo Armado que usa atos que se qualificam como terroristas de acordo com a legislação nigerina.

Da investigação, IL tem usado nome falso, com identidade falsa, um número de telefone não identificado, para frequentemente enviar dinheiro da sua localização para algum destino em DOUT, uma cidade fronteiriça no sul do país, uma área relativamente segura onde muitos traficantes de todos os tipos estão localizados. Ele tem transferido fundos para a DA usando o sistema Hawala. Uma vez feita a transferência, DA recebe uma mensagem de alerta no seu telefone a indicar o depósito de fundos feito em seu nome. Recebe também um telefonema de IL a confirmar o montante de dinheiro enviado. DA retirou os fundos, depois deslocou-se à cidade fronteiriça perto da DOUT para comprar motociclos e entregá-los na zona onde IL opera.

Além dos fundos (500,000 FCFA / motociclos) destinados à compra de motociclos, DA recebe um extra de 50,000 a 60,000 FCFA (100 USD) por motociclo transportado para a fronteira noroeste do Níger.

Fonte: Níger

CAPÍTULO 4

SINAIS DE ALERTA E INDICADORES

42. Este capítulo que decorre do anterior apresenta os sinais de alerta e os indicadores observados a partir dos casos apresentados. Sinais de alerta e indicadores são atividades ou ações que sustentam certas atividades, ações, transações ou eventos, com algumas anomalias que levantam suspeitas e/ou inconsistências quando submetidos a um escrutínio racional. Estas anomalias ou inconsistências levam a suspeitas que requerem um exame mais aprofundado, interrogatório, investigação ou, pelo menos, monitorização por parte das entidades sujeitas, dos supervisores e do público. Há uma série de indicadores e possíveis sinais de alerta que foram identificados a partir da análise dos casos apresentados no capítulo anterior. Os indicadores e sinais de alerta diferem consoante a dimensão das atividades de branqueamento de capitais ou de financiamento do terrorismo. Enquanto os indicadores representam acontecimentos que podem ou não indicar a existência de branqueamento de capitais ou de financiamento do terrorismo, os sinais de alerta representam acontecimentos que apresentam provas fortes ou mais claras de branqueamento de capitais ou de financiamento do terrorismo.

43. A seguir, encontra-se uma lista, não exaustiva, de indicadores e sinais de alerta que foram identificados a partir da análise dos casos completos. Os indicadores e sinais de alerta confirmam que a informalidade, a falta de sensibilização do público para as ameaças cibernéticas, os recursos inadequados investidos em cibersegurança por parte de empresas e instituições/organizações públicas, a fraca arquitetura e sistemas regulatórios e de monitorização do panorama cibernético na região, e os fracos sistemas de aplicação da lei têm um efeito espiral sobre a cibercriminalidade e a cibercriminalidade, branqueamento de capitais e financiamento do terrorismo na África Ocidental.

Indicadores

- O cliente empresarial com uma relação estabelecida altera os dados da conta do beneficiário (por exemplo, código IBAN) de um beneficiário conhecido.
- Existe um desfasamento entre o nome do beneficiário nas instruções de pagamento e nos dados da conta (por exemplo, código IBAN).
- Uso de serviços informais de remessas (como os serviços do tipo “Hawala”) para as transferências transfronteiras.
- Desfasamento entre a atividade económica e o fundo em questão, quer para efeitos de remessas quer para operações bancárias.
- Diferenças na grafia do nome do beneficiário em relação ao que consta nos documentos de identificação apresentados para os levantamentos.
- Utilização de serviços de transferência de dinheiro ou de valores ou de prestadores de remessas para receber fundos de clientes não relacionados.
- Utilização de “mulas” (testas de ferro), contas de por procuração, “correios”, etc., na movimentação de fundos.
- A conta do beneficiário pode pertencer a uma empresa offshore ou ser detida por uma instituição financeira localizada numa jurisdição de alto risco, conforme determinado pela instituição financeira e pelas autoridades competentes relevantes.
- Suposto pacote de um amigo *on-line* que implica pagar determinado valor antes de recebê-lo.

- Ser instruído a investir através de dinheiro móvel numa empresa suspeita que não esteja registada ou não tenha escritório físico no país.
- O cliente solicita que uma transação (pagamento) seja realizada com urgência ou solicita que a mesma seja tratada como confidencial.
- As instruções de pagamento são recebidas de um novo funcionário do cliente corporativo.
- Transações incomuns e de alto valor são solicitadas apenas por e-mail
- Pedidos de alteração para uma conta bancária do beneficiário feitos logo após uma ordem/encomenda inicial (especialmente se feita por e-mail)
- O cliente corporativo com uma relação estabelecida solicita que um pagamento seja feito a um beneficiário suspeito "pela primeira vez".
- A transação está relaconada à compra ou venda da moeda virtual (por exemplo, Bitcoins, Litecoin, Ethereum, Zcash) ou ativos virtuais semelhantes.
- O cliente solicita que uma transação seja realizada com urgência ou que seja tratada como confidencial, especialmente se imediatamente antes do horário de encerramento, fins de semana ou feriados.
- Levantamentos de dinheiro, ou operações que desembolsam um montante recebido, efetuados pouco depois de um depósito de um montante recebido do estrangeiro, ou usando um título pouco claro ou incommun.
- O cliente que solicita um pagamento a um beneficiário apenas comunica com o beneficiário via e-mail
- Operação que resulta numa atividade significativa, mas inexplicável, na conta que anteriormente estava maioritariamente inativa/tinha um baixo volume de negócios

Sinais de alerta

- Remessas regulares de vários remetentes para o mesmo destinatário ou pessoas relacionadas, incluindo remessas de um ou mais remetentes em países diferentes para um destinatário local. Particularmente, quando o destinatário não tem qualquer relação com os remetentes.
- Remessas num curto período de tempo e estruturadas logo abaixo do limiar exigido para uma comunicação mas que, em conjunto, representam uma grande soma de dinheiro.
- Entrada súbita de fundos em numerário seguida de saída súbita através de instrumentos financeiros, tais como cheques.
- Uma instituição financeira recebe uma transferência bancária para crédito numa conta. No entanto, a transferência bancária nomeia um beneficiário que não é o titular da conta registada. Isso pode refletir casos em que uma vítima envia involuntariamente transferências eletrónicas para um novo número de conta fornecido por um criminoso que se faz passar por um beneficiário, fornecedor ou vendedor conhecido.
- Utilização de serviços de remessa para o pagamento de bens e serviços encomendados online.
- Mensagem enviada sob o disfarce de uma promoção de telecomunicações e o destinatário é solicitado a inserir o seu PIN como medida de verificação para reclamar o seu "prémio".
- Receber um SMS que indica um depósito feito na conta de um cliente, posteriormente receber chamadas a dizer que o depósito foi um erro e enviar esse montante de volta.
- Receber chamada de uma empresa de entregas sob o pretexto de entregar mercadorias de amigos/parentes no estrangeiro. Você é então instruído a fazer um depósito em uma conta de dinheiro móvel para o serviço de entrega.

- Proposta de negócio atraente e boa demais para ser verdadeira de um suposto conhecido que quer que você substitua um fornecedor de produtos locais que estão em alta demanda no exterior.
- Pedido para participar ou investir em negócios que atraem retornos super normais
- Receber um e-mail com um link a sugerir que a sua conta foi pirateada/violada, ou suas fotos nuas estão na internet, ou seu ente querido precisa de cuidados de saúde imediatos, ou algum outro tipo de chantagem / ataque cibernético está prestes a acontecer e você deve seguir certas instruções, incluindo clicar no link que lhe foi enviado.
- Um pedido incomum de um amigo / parente pedindo ajuda financeira de emergência e vocês devem se comunicar apenas por mensagem.
- Mensagens relacionadas a admissão, o recrutamento de emprego ou a conquista de um prémio de um jogo online no qual você não participou, podem ser um ataque de phishing ou mesmo o recrutamento para um grupo terrorista.
- Pedidos recebidos a solicitar para atualizar os seus dados pessoais associados a informações bancárias e afins.
- Uma conta de dinheiro móvel recebe ou envia subitamente grandes somas de dinheiro, o que não corresponde à atividade anterior.
- Os fundos são imediatamente levantados ou transferidos para várias contas poucos minutos após a receção.
- Uma série de transferências de fundos de uma carteira ou conta para várias contas ou carteiras em intervalos curtos.

CAPÍTULO 5

QUADRO JURÍDICO, REGULAMENTAR, DE SUPERVISÃO E DE EXECUÇÃO/REPRESSÃO E DESAFIOS ASSOCIADOS

44. Nos últimos anos, a África Ocidental tem experimentado um aumento tremendo no seu ciberespaço e no uso do espaço, levando ao crescimento de negócios, lucros e rentabilidade e eficiência na implementação e aplicação de programas. A região também tem sofrido com um aumento exponencial na cibercriminalidade, em particular, dos crimes cibernéticos. No entanto, a taxa de deteção e prevenção pelas autoridades policiais é muito baixa. Este capítulo tenta analisar o quadro jurídico, regulamentar e de supervisão e os desafios subjacentes às medidas de execução/repressão e controlo nas economias da África Ocidental. Além disso, destaca-se a situação dos países na aplicação dos instrumentos internacionais existentes em matéria de cibercriminalidade, em conformidade com as Normas do GAFI no âmbito da Recomendação 36, que incentiva os países a ratificarem outras convenções internacionais relevantes.

Quadro Jurídico, Regulamentar e de Repressão para a Cibersegurança / Cibercrime na África Ocidental

45. Existem lacunas legislativas significativas em alguns países, particularmente em relação aos poderes da autoridade central responsável pela luta contra a cibercriminalidade e aos quadros jurídicos e de execução/repressão dos países com vista a detetar, provar e travar eficazmente o branqueamento de capitais ou o financiamento do terrorismo associados à cibercriminalidade. Apesar do quadro jurídico e de execução/repressão prever medidas de aplicação da lei para investigar e processar os cibercriminosos, o quadro regulamentar na maior parte da África Ocidental tem medidas preventivas insuficientes ou é globalmente fraco. Embora poucos países tenham conseguido alguns ganhos na obtenção de provas eletrónicas e digitais durante a investigação, este continua a ser um desafio em algumas jurisdições.

46. Um dado útil para as autoridades competentes é a forma como a legislação penal em vigor e as Normas do GAFI (que são neutras do ponto de vista tecnológico) são aplicáveis no domínio da cibercriminalidade. Isso inclui o reconhecimento da forma como as categorias de infrações existentes (no âmbito da R.3) são aplicáveis, bem como as medidas preventivas/quadro regulamentar em vigor para as IFs, as APNFDs e os prestadores de serviços de ativos virtuais. Por exemplo, em muitos dos estudos de caso, no Capítulo 3, fica muito claro que as categorias de crimes existentes, como a fraude, o roubo, a extorsão, a falsificação, a exploração sexual, etc., são aplicáveis em casos de cibercriminalidade.

47. O reconhecimento da aplicabilidade dos instrumentos e Normas existentes é importante, o que mostra que as autoridades competentes podem agir, quando aplicável, enquanto aguardam a promulgação de novas leis e regulamentos. Este reconhecimento é também importante para incentivar a colaboração transnacional, em especial no âmbito de quadros com dupla criminalização.

48. O quadro que segue apresenta as leis, regulamentos, diretivas e orientações relevantes em matéria de cibersegurança/cibercriminalidade, proteção de dados e legislação, regulamentos, diretivas conexos de LBC/CFT, tal como apresentados pelos especialistas dos Estados membros.

Quadro 3.1: Leis, Regulamentos e Diretivas sobre Cibersegurança / Cibercrimes na África Ocidental

Estados membros	Leis e Disposições Regulamentares	Observações
Benim	Lei nº 2017-20, de 20 de abril de 2018, relativa ao Código Digital; Lei nº 2018-16, de 28 de dezembro de 2018, sobre o Código Penal no Benim nos seus artigos 161º sobre atos de terrorismo, 162º-3º relativos a computadores, 670º a 689º relativos a crimes cibernéticos informáticos; Lei nº 2012-15, de 18 de março de 2013, relativa ao Código de Processo Penal; Lei nº 2011-20, de 12 de outubro de 2011, relativa ao combate à corrupção e outros crimes conexos;	O Benim tem um Código Digital que pune o cibercrime e suas possíveis consequências quando os seus autores utilizam ou não métodos para ocultar a fonte criminosa dos seus rendimentos. O Código Penal, em todas as suas disposições, prevê penas para punir os crimes de branqueamento de capitais e financiamento do terrorismo associados a cibercrimes. A lei sobre a luta contra a corrupção e outras infrações conexas sanciona infrações de financiamento de capital, financiamento do terrorismo relacionadas à cibercriminalidade.
Burkina Faso	Lei nº 001-2021/AN, de 30 de março de 2021, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais; Lei nº 040-2019/AN, de 29 de maio de 2019, relativa ao Código de Processo Penal; Lei nº 005-2017/AN, de 19 de janeiro de 2017, relativa à criação, organização e funcionamento de centros judiciários especializados na repressão das infrações económicas e financeiras e do crime organizado; Lei nº 016-2016/AN, de 3 de maio de 2016, de luta contra o branqueamento de capitais e o financiamento do terrorismo; Lei nº 061-2008/AN, de 27 de novembro de 2008, relativa ao regulamento geral das redes e serviços de comunicações eletrónicas; Portaria nº 2020-0099/PRES/PM/MSECU/ MJ/ MINEFID, de 14 de fevereiro de 2020, sobre a criação, competências, organização e funcionamento da Brigada Central de Combate ao Cibercrime; Portaria nº 2013-149/PRES/PM/MDENP/MEF/MJ, de 21 de março de 2013, que define as obrigações dos operadores de serviços de comunicações eletrónicas no que respeita à conservação de dados de tráfego e de localização; Portaria nº 2013-1053/PRES/PM/MEF/MATS, de 11 de novembro de 2013, que cria a Agência Nacional de Segurança dos Sistemas de Informação.	A luta contra a cibercriminalidade tem sido objeto de uma série de textos tendentes fornecer o necessário enquadramento. Em termos de textos legislativos e regulamentares, registamos a adoção de um certo número de textos que regula e pune as infrações relacionadas com a cibercriminalidade.

Estados membros	Leis e Disposições Regulamentares	Observações
Cabo Verde	O Decreto-Lei nº 9/2021, de 29 de janeiro, criou o regime jurídico da cibersegurança e a equipa de resposta a incidentes de segurança informática; Criação da Lei do Cibercriminalidade nº 8/IX/2017, de 20 de março - relativa à cooperação internacional em matéria penal e à recolha de provas em formato eletrónico; Regime Geral de Proteção de Dados pela Lei n.º 41/VIII/2013, de 17 de setembro; Lei sobre o Comércio Eletrónico; Lei das Infraestruturas Públicas chave; Lei sobre a Assinatura Digital; Lei da Identidade Electrónica.	Cabo Verde estabelece as disposições penais, materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao combate à cibercriminalidade e à recolha de provas digitais e dados eletrónicos.
Cote d'Ivoire	Lei nº 2013-451, de 19 de junho de 2013, relativa à luta contra a cibercriminalidade; Lei nº 2013-450, de 19 de junho de 2013, relativa à proteção de dados pessoais; Lei nº 2011-546, de 30 de julho de 2013, relativa às transações eletrónicas que regem o comércio eletrónico, a publicidade, etc.; Portaria nº 2012-243 que rege todas as atividades de TIC de ou para a Côte d'Ivoire; e o Decreto nº 2011-476, de 21 de dezembro de 2011, que identifica os assinantes dos prestadores de serviços de telecomunicações.	Esta lei define infrações específicas relacionadas com as TIC, infrações à propriedade intelectual, atos ilegais nas redes de comunicações eletrónicas e as responsabilidades dos prestadores de serviços em linha. Adapta as infrações tradicionais às TIC e clarifica o processo penal para a cibercriminalidade. Além desta, outras leis, regulamentos e decretos foram emitidos, além do código penal, pelas autoridades marfinenses com o objetivo de regular e proteger o ciberespaço marfinense.
Gâmbia	Lei da Informação e das Comunicações (ICA), 2009; Lei da Prova, 1994; Lei de Direitos Autorais, 2004; Projeto de Lei das Infrações Penais, 2020; Código Penal (1933, com a última redação que lhe foi dada pela Lei nº 18 de 2010); Código de Processo Penal (1933, com a última redação que lhe foi dada pela Lei nº 5 de 2005;	O Conselho da Europa e o OCWAR-C apoiaram o Ministério da Justiça e o Ministério da Economia Digital das Comunicações da Gâmbia na preparação de um projeto de lei sobre cibercrimes, que foi finalizado em dezembro de 2019 e aberto a consulta pública até janeiro de 2020. O Ministro das Comunicações e da Economia Digital ainda está a trabalhar na finalização do projeto de lei sobre cibercrimes.

Estados membros	Leis e Disposições Regulamentares	Observações
Gana	Lei de Segurança Cibernética, 2020 (Lei 1038); Lei da Agência Nacional de Tecnologia da Informação (NITA), 2008 (Lei 771); Lei de Transações Eletrónicas, 2008 (Lei 772); Lei das Comunicações Eletrónicas, 2008 (Lei 775); Lei de Proteção de Dados, 2012 (Lei 843); Lei do Gabinete de Crimes Económicos e Organizado, 2010 (Lei 807); Lei de Luta contra o Branqueamento de Capitais, 2020 (Lei 1044); Lei de Combate ao Terrorismo, 2008 (Lei 762); Lei dos Sistemas e Serviços de Pagamentos de 2019 (Lei 987); Lei relativa ao Auxílio Judiciário Mútuo, 2010 (Lei nº 807); Lei relativa aos bancos e às instituições depositárias especializadas de 2016 (Lei nº 930); Lei das Instituições Financeiras Não Bancárias de 2008 (Lei 774).	O Lei da Cibersegurança procura promover o desenvolvimento da cibersegurança e prever questões conexas. Também criou a Autoridade de Cibersegurança (CSA) para regular as atividades de cibersegurança. O conselho dessa autoridade é constituído pelos ministros das Comunicações, da Defesa, da Segurança Nacional e do Interior. Para uma boa coordenação em matéria de incidentes de cibersegurança, a autoridade é obrigada a criar equipas setoriais de resposta a emergências informáticas (CERT), incluindo para os setores bancário e financeiro.
Guiné	Lei L/037/AN/2016 relativa à cibersegurança e à proteção de dados pessoais; Lei L/035/AN/2016 relativa às transações eletrónicas; Lei nº 059/AN/2016 do Código Penal; Lei L/2021/024/AN, de 17 de agosto de 2021, relativa ao combate ao branqueamento de capitais e ao financiamento do terrorismo.	As leis definem as regras e mecanismos de combate a cibercrimes e, assim, criam um ambiente favorável, propício e seguro no ciberespaço, mas também para permitir que a República da Guiné cumpra os seus compromissos comunitários e internacionais em matéria de cibersegurança. Promove igualmente a modernização da utilização das TIC e apoia a luta contra o BC/FT.
Libéria	Lei da Fraude, 2012 – criminaliza a fraude eletrónica e a fraude postal. Lei de Medidas Preventivas de LBC/CFT relativas aos Produtos do Crime 2021- reconhece a fraude como uma infração subjacente ao BC.	A Libéria como país não tem uma legislação específica sobre cibercrimes. Um projeto de lei (Lei sobre Cibercrimes) foi submetido ao Parlamento para promulgação. No entanto, a Libéria baseia-se noutros diplomas legislativos para lidar com questões relacionadas com cibercrimes.

Estados membros	Leis e Disposições Regulamentares	Observações
Nigéria	Lei sobre Cibercrimes (Proibição, Prevenção, etc.), 2015; Lei relativa à Comissão de Crimes Económicos e Financeiros (Criação), 2004; Lei relativa à fraude de pagamentos adiantados e outras infrações conexas, 52 (2006); a Lei de Branqueamento de Capitais (Proibição), de 2011, alterada em 2013; a Lei Nigeriana sobre Provas, a Lei do Código Penal, a Lei do Código Penal, a Lei do Terrorismo (Prevenção), de 2013, e a Lei da Comissão Nacional de Gestão da Identidade, de 2007	Com a Lei relativa a Cibercrimes em 2015, a Nigéria tornou-se mais equipada da jurdicamente na luta contra as atividades do cibercrime. No entanto, pode não ser adequado discutir a Lei do Cibercrime de 2015 sem lançar alguma luz sobre as leis facilitadoras que existiam para controlar os crimes cibernéticos (ou seja, a Lei da EFCC, a Lei de AFF, etc.) antes dessa Lei ser promulgada.
Senegal	Lei 2008-08 relativa às transações electrónicas e à promoção do comércio de TIC; Lei 2008-12 de 25 de janeiro de 2008, sobre a proteção de dados pessoais; lei 2008-11 de 25 de janeiro de 2008 sobre cibercrimes;	Já em 2008, o país adotou um quadro normativo para combater o cibercrime e regular o sistema de informação. Estas leis fornecem o quadro relativo às transações eletrónicas, ao tratamento de dados, promovem o desenvolvimento do comércio no setor das TIC e a proteção dos dados pessoais, bem como o respeito pelos direitos humanos e liberdades fundamentais.
Serra Leoa	Lei das Telecomunicações de 2006; Lei de Cibersegurança e Cibercrimes 2021; Lei de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo de 2012; Lei de Segurança Nacional e Informações Centrais de 2002.	Esta lei estabelece um quadro para travar a cibercriminalidade, o branqueamento de capitais e o financiamento do terrorismo, proteger estruturas de informação e sistemas informáticos nacionais críticos, recolher provas eletrónicas para investigar e processar os cibercrimes, proteger a segurança nacional, realizar operações encobertas de informação em todo o território da Serra Leoa e facilitar a cooperação internacional.

49. O Quadro 3.1 apresenta as disposições legais e regulamentares adotadas pelas autoridades competentes dos Estados membros para combater a cibercriminalidade. Com exceção de alguns que ainda dependem de outras leis relacionadas para combater o cibercrime, a maioria dos Estados membros tem leis autónomas em matéria de cibersegurança e cibercriminalidade. A aplicação desta lei à deteção, investigação e ação penal centrou-se principalmente na infração subjacente, ignorando a necessidade de deteção e de investigações paralelas do aspeto do branqueamento de capitais dos casos.

Instituições responsáveis pela luta contra a cibercriminalidade na África Ocidental

Benim

50. O organismo líder na luta contra a cibercriminalidade é o Escritório Central de Repressão da Cibercriminalidade (OCRC), que está sob a tutela do Diretor da Polícia Judiciária, sendo responsável por assegurar que todas as medidas preventivas são consideradas no combate à cibercriminalidade, incluindo as infrações relacionadas com os sistemas informáticos, bem como a gestão das bases de dados. Também presta assistência técnica a serviços que requerem a sua especialização, realiza formação, etc. A UIF é também responsável pela análise da informação e pelo fornecimento da origem, destino, natureza de eventuais operações, etc. Outras instituições responsáveis pelo combate ao cibercrime são o Ministério da Economia e Finanças, o Ministério da Justiça, o Ministério do Interior e da Segurança Pública, a Agência Nacional de Identificação de Pessoas (ANIP), a Agência de Sistemas de Informação e Digitais, a Agência de Desenvolvimento Digital (DNA) e a Agência Beninense de Comunicações Eletrónicas Universais e Serviço Postal (ABSUCEP).

Burkina Faso

51. O Ministério da Transição Digital, Correios e Comunicações Eletrónicas (MTDPCE) assegura a implementação e monitorização da política governamental em termos de desenvolvimento da economia digital, correios e transformação digital. A Agência Nacional de Informações tem como principais missões recolher e explorar informações reconhecidas como de interesse vital para a segurança. A Comissão de Informática e Liberdades (CIL) é a autoridade de supervisão responsável por assegurar a proteção dos dados pessoais, informando todos os titulares dos dados e controladores de dados dos seus direitos e obrigações e controlando a utilização das tecnologias de informação e comunicação aplicadas ao tratamento de dados pessoais. A Agência Nacional de Segurança dos Sistemas de Informação (ANSSI) é responsável pela gestão da segurança dos sistemas de informação e do ciberespaço. A Autoridade Reguladora das Comunicações Eletrónicas e dos Correios (ARCEP) é responsável por monitorizar a conformidade com a regulamentação em vigor no setor das comunicações eletrónicas, por gerir e atribuir radiofrequências e monitorizar as condições de utilização, monitorar o desenvolvimento de tecnologias e prescrever medidas para estimular e facilitar o investimento no setor das comunicações eletrónicas. A Célula Nacional de Tratamento de Informação Financeira (CENTIF) é responsável pela recolha, tratamento e divulgação de informações às autoridades competentes ou outras unidades de informação financeira. Outros atores estatais são a Direção-geral da Polícia Nacional, o Estado-Maior da Gendarmerie Nacional, a Direção-Geral de Transmissões e TI, a Brigada Central de Combate aos Cibercrimes, a Brigada Especial de Investigações de Combate ao Terrorismo e Luta contra o Crime Organizado, o Gabinete de Identificação Nacional e o Ministério da Justiça.

Cabo Verde

52. Cabo Verde continua a investir fortemente numa sociedade do conhecimento, informativa, inovadora e próspera, bem como a investir e reforçar as instituições de TIC, nomeadamente a Agência Reguladora Multissetorial da Economia, o Ministério da Economia Digital, o Conselho Nacional para o Desenvolvimento das TIC na Comissão Nacional de Proteção de Dados e na disponibilização de infraestruturas tecnológicas de qualidade, bem como na formação de recursos humanos. O Governo aprovou a Estratégia Nacional de Cibersegurança (ENCS) e criou o Núcleo Nacional de Cibersegurança (NNCS). O Governo criou ainda, em 2021, a Equipa de Resposta a Emergências Informáticas e a Brigada Central de Combate ao Cibercrime e ao Terrorismo da Polícia Judiciária - BCCCT.

Côte d'Ivoire

53. Os intervenientes estatais que estão na linha da frente do combate ao cibercrime é a Direção de Rastreio das TI (DITT) é uma entidade da Polícia Nacional com serviços especializados responsáveis pelas infraestruturas de telecomunicações e prestação de assistência técnica aos serviços policiais e judiciais. Esta estrutura foi criada em maio de 2007 no âmbito da luta contra a cibercriminalidade. A Equipa de Resposta a Emergências Informáticas (CI-CERT) foi criada pela Autoridade Reguladora das Telecomunicações em junho de 2009. É um centro de alerta e resposta de emergência para ataques cibernéticos que ocorrem no ciberespaço da Côte d'Ivoire. Dotada de recursos humanos especializados em sistemas de segurança da informação, a equipa oferece assistência técnica proativa e reativa a empresas e particulares durante falhas de segurança. Como centro de coordenação com uma rede de parceiros globais, é o ponto focal nacional para monitorização, deteção e alerta de segurança de TI. O fórum sobre a luta contra a cibercriminalidade é também um acordo de parceria assinado em 2011, e atualizado em 2014, entre a Direção-Geral da Polícia Nacional e o CI-CERT. É uma entidade integrada no DITT da Polícia Nacional que assegura a sua gestão. O PLCC é outra estrutura responsável pela luta contra o cibercrime no país e é apoiado na execução das suas missões pelo CI-CERT e pelo Laboratório Forense Informático do DITT. Além de investigações criminais que incluem a busca e a prestação de justiça para suspeitos de cibercriminosos.

54. Outros intervenientes estatais na luta contra a cibercriminalidade são a UIF, a Agência de Gestão e Recuperação de Bens Criminais (AGRAC), a Direção de Polícia Económica e Financeira, a Unidade de Criminalidade Económica e Financeira, um tribunal criminal de primeira instância especializado em criminalidade económica e financeira, o Ministério Público, a Direção de Polícia Criminal e as seções de investigação da Gendarmerie Nacional. Os intervenientes não estatais são as empresas de telecomunicações, os operadores de telemóveis, os fornecedores de serviços de Internet e as instituições financeiras.

A Gâmbia

55. O Ministério das Comunicações e da Economia Digital supervisiona o desenvolvimento e a implementação das leis, regulamentos e estratégias para o setor das TIC. O setor das telecomunicações, uma componente essencial da infraestrutura nacional crítica da Gâmbia, é amplamente regulado pela Autoridade Reguladora dos Serviços Públicos («PURA»). PURA cria a Equipa de Segurança Informática e Resposta a Incidentes da Gâmbia (gmCSIRT). O gmCSIRT suporta todos os detentores de Infraestruturas Críticas de Informação (CII) na Gâmbia. Os Gabinetes do Procurador-Geral e o Ministério da Justiça, através do Departamento do Ministério Público, são responsáveis por iniciar, assumir e acusar ou arquivar os processos penais contra ou em relação a qualquer infrator. O poder judicial da Gâmbia detém o mandato geral para a resolução de litígios através do devido processo legal, administração de tribunais, registos, processos, diretivas e procedimentos e execução de decisões, ordens, sentenças e decisões judiciais. A Força Policial da Gâmbia também está na vanguarda do combate aos crimes cibernéticos. A polícia beneficiou através do projeto OWAR C de um Laboratório Digital equipado e cerca de (15) agentes da polícia receberam formação sobre como conduzir a investigação forense digital em dispositivos e redes eletrónicos para conduzir com sucesso investigações de cibercrimes. A UIF está mandatada para realizar análises, divulgar ou arquivar Comunicações de Operações Suspeitas (COS), procurando/respondendo a pedidos de informação. A Gâmbia estabeleceu uma Aliança de Segurança Cibernética (GCSA) em 2017 e desenvolveu um Plano Nacional de Cibersegurança (2020 a 2024) que serve como guia para a proteção dos sistemas de informação do país, as infraestruturas críticas e o ciberespaço da Gâmbia em geral.

Gana

56. Os intervenientes estatais responsáveis pela luta contra a cibercriminalidade no Gana são o Centro de Informação Financeira (UIF), a Unidade de Cibercrime do Departamento de Investigação Criminal do Serviço de Polícia do Gana, o Escritório da Criminalidade Económica e Organizada (EOCO), a Autoridade Nacional do Ciberespaço, o Gabinete Nacional de Informações (NIB), a Autoridade Nacional de Comunicações (NCA), o Banco do Gana (BoG) e a Comissão de Valores Mobiliários (SEC). O Ministério das Comunicações e Digitalização (MOCD),

usando o Cartão de Gana como documento de origem, anunciou o novo registo de cartões Módulo de Identificação de Subscritores (SIM) oferecidos pelas empresas de telecomunicações no país. O Centro Nacional de Cibersegurança do MOCD é responsável pela capacitação e pela sensibilização do público em geral em matéria da ciber-higiene e a cibersegurança.

Libéria

57. A Autoridade de Telecomunicações da Libéria (LTA) é responsável por licenciar e regular operadores de telecomunicações, prestadores de serviços e monitorizar o seu desempenho, implementa políticas e estratégias relativas aos serviços de telecomunicações e elabora a agenda política para o desenvolvimento das TIC e Telecomunicações na Libéria. A Agência Nacional de Segurança (NSA) tem um laboratório de cibercrime, mas as diretivas para a notificação e acessibilidade ao público para denunciar casos de cibercrime são desconhecidas. A Polícia Nacional da Libéria (LNP) tem uma seção para lidar com casos de cibercrime, mas está inativa, com poucos recursos humanos, falta de conhecimentos e ferramentas sobre cibercrime. A Agência de Informação Financeira (FIA) funciona como a agência central nacional responsável pela receção e análise de comunicações de operações ou de atividades. A Agência de Prevenção e Mitigação de Crimes Cibernéticos da Libéria (LCCPMA), como instituição também tem vastas redes de apoio internacionais, algumas das quais incluem parceria com a *Global Cyber Alliance* em 2020 e com o *Global Forum on Cyber Expertise* (GFCE) em 2021, etc.

Nigéria

58. Os quadros institucionais discutidos são a Unidade de Informação Financeira da Nigéria (NFIU), a Unidade Especial de Controlo contra o Branqueamento de Capitais e o Grupo de Trabalho sobre Cibercrime da Nigéria. A cibercriminalidade é um termo que descreve amplamente a atividade criminosa em que os computadores ou as redes informáticas são uma ferramenta, um alvo ou um local para a atividade criminosa. Com o fácil acesso à Internet, a cibercriminalidade tornou-se cada vez mais prevalente entre os nossos jovens de hoje. O que é mais preocupante é o ritmo em que as suas vítimas caem nos truques fraudulentos. O que é ainda mais preocupante é que estes jovens dominaram o ato do cibercrime.

Senegal

59. Para conter os impactos do cibercrime e questionar os executivos e as ferramentas necessárias para entender o ambiente digital, o Senegal criou uma escola nacional de cibersegurança com vocação regional em 2018. Esta escola tem como principal objetivo proporcionar a formação de especialistas em cibersegurança e constituir um polo de referência em África. Por último, para adaptar as suas organizações e dotar-se dos meios necessários para responder eficazmente aos desafios de segurança impostos pela cibercriminalidade, a Polícia Nacional e a Gendarmerie criaram serviços especializados na luta contra a cibercriminalidade. Trata-se, respetivamente, da Divisão Especial de Cibersegurança (DSC) e da Plataforma Digital de Combate ao Cibercrime (PNLC).

Guiné

60. A Agência Nacional para a Segurança dos Sistemas de Informação (ANSSI) é um interveniente importante no domínio da cibersegurança e presta conhecimentos especializados e assistência técnica a reguladores, agências de aplicação da lei e empresas. Presta serviços de monitorização, deteção, alerta e reação a ciberataques. A Unidade de Cibercriminalidade da Direção Central da Polícia Judiciária é também um organismo criado pelo Ministro da Segurança e Proteção Civil e desempenha um papel muito importante no combate à cibercriminalidade. A Divisão de Investigações Criminais da Direção Central da Polícia Judiciária é também responsável pelas investigações de cibercriminalidade e trabalha em estreita colaboração com todos os magistrados do Ministério Público do país. Outros intervenientes estatais são a autoridade reguladora dos correios e telecomunicações, a Agência Nacional de Luta contra a Corrupção e a Promoção da Boa Governação (ANLC), a Unidade de Informação Financeira, a Rede Central da INTERPOL (BCN) e o Ministério Público.

Serra Leoa

61. A Unidade de Cibercriminalidade investiga todos os casos de cibercriminalidade denunciados. A Comissão Nacional de Telecomunicações (NATCOM) é o principal regulador de todos os serviços de telefonia móvel e provedores de serviços de internet (ISPs). Emite diretivas e orientações e colabora com os investigadores da cibercriminalidade e a UIF. A UIF fornece análises financeiras e relatórios analíticos de informação financeira sobre as atividades de BC/FT, se necessário. Outros atores estatais são a Autoridade Nacional de Registo Civil (NCRA), a Unidade de Crime Organizado Transnacional (TOCU), a Unidade Central de Informações Estratégicas e Segurança (CISU), a Polícia de Serra Leoa e o Diretor do Ministério Público (DPP). Para além destes intervenientes estatais, existem iniciativas de colaboração interagências, como o Conselho Consultivo Nacional de Cibersegurança, o Grupo de Trabalho Técnico Nacional de Cibersegurança, o Grupo de Trabalho sobre Crimes Financeiros e o Comité Conjunto de Informações. Estes organismos são constituídos pelos intervenientes das agências responsáveis pela aplicação da lei, das instituições reguladoras, das instituições de segurança e de recolha de informações e dos ministérios competentes. O principal objetivo destas estruturas interagências é alcançar um elevado nível de cooperação e colaboração, a fim de garantir um ambiente cibernético seguro. Serra Leoa também desenvolveu uma Estratégia Nacional de Cibersegurança e Proteção de Dados (2017 – 2022). A estratégia classifica a cibercriminalidade em ciberdependentes (crimes cometidos apenas com a utilização de dispositivos TIC, em que os dispositivos são simultaneamente o instrumento para cometer o crime e o alvo do crime, enquanto os cibercrimes lidam com crimes antiquados que, devido à utilização de dispositivos e redes TIC, aumentaram em escala ou alcance.

Ratificação dos instrumentos internacionais

62. Em conformidade com os requisitos das normas mundiais, em particular, a Recomendação 36 do GAFI sobre Cooperação Internacional (ou seja, a aplicação de instrumentos internacionais), "*.... os países são igualmente incentivados a ratificar e aplicar outras convenções internacionais relevantes, como a Convenção do Conselho da Europa sobre a Cibercriminalidade, de 2001; .....*". este requisito é conhecido como Convenção de Budapeste.

63. Tal como a Convenção de Budapeste, a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais (junho de 2014), conhecida como Convenção de Malabo, incentiva os seus membros a ratificarem e aplicarem as disposições estabelecidas na convenção e conforme acordado pelos membros. No entanto, os mecanismos de cooperação interinstitucional e internacional são pouco regulados pela legislação, pelo que os desafios à investigação e à ação penal neste domínio continuam a ser significativos em alguns países. Embora quase todos os países da África Ocidental tenham em vigor uma estratégia nacional para combater a cibercriminalidade, alguns deles ainda não ratificaram as Convenções de Budapeste e de Malabo para reforçar a cooperação transfronteiriça regional.

64. Segue o estado de ratificação e implementação dos dois instrumentos complementares (convenções) para ajudar os Estados membros a reforçar o seu quadro de prevenção e interrupção da cibercriminalidade.

Figura 3.1: Ratificação dos instrumentos internacionais



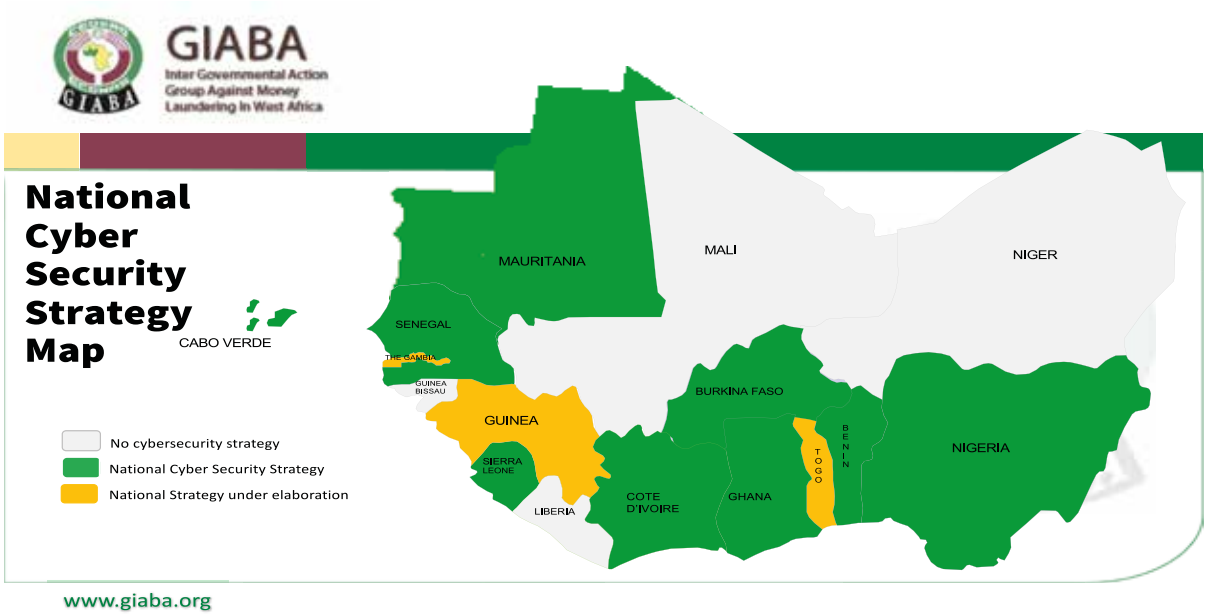
Fonte: OCWAR-C

65. A Figura 3.1 acima mostra que 4 países, Cabo Verde, Gana, Nigéria e Senegal são parte à Convenção de Budapeste, enquanto outros 5 países, Benim, Burkina Faso, Cote d'Ivoire, Níger e Serra Leoa são agora signatários e convidados a aderir à Convenção, elevando para 9 o número de países da África Ocidental que tomaram medidas para implementar a Convenção de Budapeste sobre a cibercriminalidade. No caso da Convenção de Malabo, apenas o Gana e o Togo aplicaram plenamente o requisito (assinatura e ratificação) da Convenção na África Ocidental. Além do Gana e do Togo, outros 5 países apenas ratificaram (Cabo Verde, Cote d'Ivoire, Guiné, Níger e Senegal) sem assinar a convenção, enquanto outros 3 países assinaram (Gâmbia, Guiné-Bissau e Serra Leoa) sem ratificar a convenção. Há, no entanto, 2 outros Estados membros não membros da CEDEAO GIABA que assinaram a Convenção de Malabo, mas ainda não a ratificaram.

66. Além disso, o projeto da União Europeia sobre Crime Organizado: Resposta da África Ocidental à Cibersegurança e luta contra o Cibercrime (OCWAR-C), executado pelo grupo Expertise France, trabalhou com os Estados membros para desenvolver estratégias nacionais de cibersegurança. Durante o período em análise, 8 países tinham posto em prática estratégias nacionais, com outras 3 finalizadas, elevando o total para 11 dentre os 15 países. Os outros 4 países que ainda não desenvolveram as suas estratégias nacionais de cibersegurança são a Guané-Bissau, a Libéria, o Mali e o Níger. Segue-se o mapa que mostra o estado das estratégias nacionais.

67. A nível regional, a CEDEAO emitiu uma Diretiva (2010) relativa à luta contra a cibercriminalidade e à adoção da lei e de procedimentos penal substantivos para combater a cibercriminalidade nos Estados membros. Além desta diretiva, a CEDEAO implementou a disposição de harmonização, em particular, a Lei Complementar sobre proteção de dados pessoais e garantir a confidencialidade, e a Lei Complementar sobre transações eletrônicas com condições para aceitação de assinatura eletrónica.

Figura 3.2: Estratégia Nacional de Cibersegurança na África Ocidental



Fonte: OCWAR-C

Desafios jurídicos, regulamentares e de execução

68. A região da África Ocidental envidou esforços e realizou progressos consideráveis na luta contra a cibercriminalidade, a par de outros crimes principais. Mas estes esforços e progressos não estão isentos de desafios, que continuam a ser assustadores e persistentes à medida que os criminosos engendram novos métodos e técnicas para evitar deteção. Segue-se um resumo dos desafios.

69. Embora a maioria dos Estados membros da GIABA tenha tomado medidas para ter leis para capacitar as autoridades competentes na luta contra o cibercrime, ainda existem limitações no quadro jurídico e institucional existentes. Há zonas cinzentas que precisam ser alinhadas adequadamente, onde existam leis, e os países sem leis autónomas devem acelerar o processo para as promulgar. As leis devem orientar-se pelas disposições das convenções de Budapeste e de Malabo, incluindo a aceitação de provas digitais e eletrónicas nos tribunais para acelerar os processos judiciais. As Normas do GAFI também preveem medidas relevantes através de várias recomendações (particularmente a R.3 e outras recomendações que tratam de medidas preventivas para IFs, APNFDs e VASPs).

70. O baixo nível de operacionalidade das estruturas e mecanismos responsáveis pela cibersegurança e pela luta contra a cibercriminalidade. É necessário reforçar a criação de um laboratório digital, dotado de instrumentos de elevado desempenho para analisar provas digitais e utilizar eficazmente essa tecnologia ao longo de toda a cadeia de justiça penal. É necessário definir claramente os papéis e as responsabilidades dos diferentes intervenientes e compreender as modalidades de colaboração e coordenação.

71. A especialização/conhecimento das autoridades competentes no combate à cibercriminalidade em investigações financeiras e digitais é ainda muito básica/baixa e exige formação contínua destes intervenientes (polícia, procuradores, engenheiros de TIC, analistas da UIF, magistrados e todos os intervenientes na cadeia da justiça penal).

72. A insuficiência de recursos (financeiros e materiais) continua a retardar a luta contra a cibercriminalidade, uma vez que os casos são frequentemente comunicados em números e os registos a considerar para análise são, na sua maioria, volumosos e exigem competências e recursos humanos. Por exemplo, quando milhões de registos, contas, cartões de crédito ou fotos pessoais são pirateados, você precisa de um bom número de pessoal altamente qualificado para concluir a investigação em tempo hábil.

73. Falta de consciência dos perigos da falta de precauções e da utilização inadequada do ciberespaço, incluindo as redes sociais. Sensibilização inadequada dos utilizadores das TIC e das vítimas de cibercrimes quanto ao seu direito de apresentar queixas. Além disso, os cibercriminosos são encorajados devido ao facto de a maioria das vítimas, especialmente quando se trata de certos crimes que afetam a honra e a dignidade, se absterem de apresentar queixas e preferirem resignar-se à sua sorte, a fim de evitar qualquer escândalo ou estigma.

74. Falta de colaboração interinstitucional e de cooperação internacional. A ratificação das Convenções de Budapeste e Malabo sobre a cibercriminalidade é ainda muito reduzida, tal como o são os benefícios daí decorrentes em termos de cooperação internacional e de reforço das capacidades. A intensificação da cooperação inter-agências para uma melhor gestão dos dados e informações que possam conduzir à deteção de infrações, à detenção dos presumíveis autores e ao seu encaminhamento para os ministérios públicos competentes.

75. A natureza complexa da investigação necessária para reunir provas para processar casos cibernéticos é um grande obstáculo. A maior dificuldade enfrentada pelas autoridades policiais reside na identificação da principal fonte do ciberataque. A Unidade de Cibercriminalidade e outras Unidades de Aplicação da Lei são muitas vezes incapazes de chegar à fonte da informação, mesmo dentro do país, e é ainda mais complexo numa situação em que o ciberataque teve origem fora do país e existe a necessidade de recorrer a um pedido de auxílio judiciário mútuo.

CAPÍTULO 6

CONCLUSÃO E RECOMENDAÇÕES

Conclusão

76. A inovação e as tecnologias emergentes mudaram a forma como os negócios estão a ser conduzidos em todo o mundo. Na mesma linha, organizações e instituições adotaram formas inteligentes de implementar programas que levam à eficiência e eficácia. O mundo tem testemunhado um crescimento significativo a partir do uso dessas tecnologias emergentes, seja tecnologia financeira, inteligência artificial, inteligência de negócios, robótica, ChatGPT, etc.

77. No entanto, estas tecnologias que operam na autoestrada da Internet conhecida como ciberespaço são utilizadas para cometer, facilitar e facilitar crimes clássicos (infrações subjacentes ao BC/FT). A cibercriminalidade e o BC/FT estão intrinsicamente ligados e, juntos, representam grandes desafios em matéria de segurança em todo o mundo. De modo geral, é necessário um elevado nível de competências em TICs para cometer e combater a cibercriminalidade. No entanto, este não é o caso na África Ocidental, onde tem havido um desfasamento entre as competências superiores demonstradas pelos cibercriminosos e as das autoridades competentes que combatem a cibercriminalidade.

78. Embora exista uma vasta gama de métodos e técnicas utilizados pelos cibercriminosos para branquear o produto das suas atividades criminosas, os investigadores e os procuradores realizaram poucas ou nenhumas investigações financeiras paralelas quando é detetada a ocorrência de cibercrimes. São também confrontados, em muitos casos, com a dificuldade de estabelecer provas da infração de cibercrimes, devido à falta de tecnologias ou de equipamentos necessários, à coordenação nacional integrada ineficaz entre as unidades operacionais de LBC/CFT e à falta de implementação de mecanismos de cooperação regional e internacional.

Recomendações

79. A fim de manter firme o rumo da luta contra a cibercriminalidade na África Ocidental, tornando-a simultaneamente mais eficaz e dissuasora, são apresentadas as seguintes recomendações, tanto para o público como para as autoridades competentes que lutam contra a cibercriminalidade.

Para o público

80. Lançar e intensificar campanhas de sensibilização destinadas ao público em geral sobre o modus operandi dos cibercriminosos e os riscos associados à utilização da Internet, bem como sobre os métodos e técnicas existentes utilizados pelos cibercriminosos.

81. Promover a cultura da cibersegurança na região e apoiar os países no estabelecimento de um quadro legal e institucional de acordo com as normas internacionais atualmente em vigor.

Autoridades nacionais

82. Para combater eficazmente a cibercriminalidade, os riscos devem ser devidamente avaliados e compreendidos pelos países. Para o efeito, estatísticas fiáveis e abrangentes devem ser bem recolhidas sobre a situação real relacionada com a cibercriminalidade.

83. Criação de Laboratório Forense Digital;: provas forenses para apoiar os esforços policiais, judiciais ou de segurança para ligar um indivíduo ou indivíduos a um crime, fornecendo provas (incluindo provas digitais), detetando e monitorizando certos tipos de crime utilizando informações financeiras e inteligência artificial.

84. Reforçar as capacidades operacionais dos investigadores em técnicas de investigação digital adaptadas à investigação criminal desta categoria de infrações.

85. Colmatar a lacuna entre o quadro jurídico e as leis especiais de LBC/CFT/CFP para facilitar e acelerar a instauração de processos criminais contra os cibercrimes.

86. Estabelecer e promover mecanismos de cooperação entre as autoridades responsáveis pela aplicação da lei, os intervenientes e outras autoridades competentes.

87. Em linha com as normas do GAFI, tomar medidas que possam reforçar a cooperação transfronteiriça, fazendo parte de outros instrumentos internacionais relevantes que permitam a cooperação internacional em casos de cibercriminalidade, como a Convenção de Budapeste sobre a Cibercriminalidade e a Convenção de Malabo.

88. Dotar as autoridades policiais competentes que combatem a cibercriminalidade de recursos suficientes (humanos, materiais, financeiros, etc.).

89. Desenvolver um Quadro Nacional de Identificação Digital para salvaguardar os Sistemas de Identificação Digital.

90. Promover juízes e procuradores especializados dedicados a processar e julgar infrações relacionadas à cibercriminalidade.

Organismos / Autoridades Regionais e Internacionais

91. Criar um Fórum Regional de Plataformas Nacionais de Combate à Cibercriminalidade na África Ocidental para permitir que as autoridades competentes estabeleçam redes, partilhem informações e relatórios analíticos, e partilhem experiências em tempo real.

92. Cooperar no seguimento e monitorização da assinatura, ratificação e incorporação na ordem jurídica interna de instrumentos internacionais. Criar um quadro de cooperação entre investigadores e unidades de cibercriminalidade.

93. Desenvolver capacidades em matéria de deteção, investigação, acusação penal e julgamento de casos de cibercriminalidade e de como seguir o rastro do dinheiro, incluindo a realização de investigações paralelas e financeiras.

94. Apoiar a realização de avaliações de riscos relacionados com o ciberespaço/cibernética, tanto nacionais como supranacionais.

REFERÊNCIAS BIBLIOGRÁFICAS

ECA (2021), 'Cybercrime, A barrier to Africa's thriving digital economy', https://www.uneca.org/stories/cybercrime%2C-a-barrier-to-africa%E2%80%99s-thriving-digital-economy

FATF – Interpol - Egmont Group (2023), 'Illicit Financial Flows from Cyber-Enabled Fraud,' https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber- enabled-fraud.html
FATF (2021), 'Opportunities and Challenges of New Technologies for AML/CFT', https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html

FATF (2022), 'Money Laundering and Terrorist Financing Arising from Migrant Smuggling' https://www.fatf-gafi.org/en/publications/Methodsandtrends/Migrant-smuggling.html

Feyen, E. et. Al (2021), 'Fintech and the digital transformation of financial services: implications for market structure and public policy', a BIA Paper No 117, https://www.bis.org/publ/bppdf/bispap117.pdf

Konellos, M. F. (2021), '*Cyber Security Challenges with Emerging Technologies'* https://www.japcc.org/articles/cybersecurity-challenges-with-emerging-technologies/

Kshetri, N. (2019), 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management, https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527

OECD (2021), 'Misuse of E-Commerce for Trade in Counterfeits', https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/misuse-e-commerce-trade-in-counterfeits/EUIPO_OECD_misuse-e-commerce-trade-in-counterfeits_study_en.pdf

Onota, E. (2021), 'Globalization and Emergence of Cyber Crimes in Nigeria: the YahooBoys Syndrome', Journal of Political Sciences & Public Affairs

Sumadinata, W. S. (2023), 'Cybercrime and Global Security Threats: A Challenge in International Law', Russian Law Journal, Volume XI (2023) Issue 3

Tropina, T. (2016), 'Do Digital Technologies Facilitate Illicit Financial Flows ?', World development report, https://thedocs.worldbank.org/en/doc/396751453906608518-0050022016/original/WDR16BPDoDigitalTechnologiesFacilitateIllicitFinancialFlowsTropina.pdf

ANEXO A:

MODELO DE FORMULÁRIO DE ANÁLISE DE CASOS

MODELO DE FORMULÁRIO DE ANÁLISE DE CASOS PARA PROJETO DE TIPOLOGIAS SOBRE BRANQUEAMENTO DE CAPITAIS E FINANCIAMENTO DO TERRORISMO LIGADO AO CIBER-CRIME NOS ESTADOS MEMBROS DO GIABA

Nome do país_____ No do Caso._____

a. **Síntese dos factos do caso (incluindo o que motivou o início da investigação e a situação do caso à data em que foi relatado):**

b. **Técnicas/métodos**

Indicar, com o exemplo do caso, a ocorrência de qualquer uma das seguintes técnicas/métodos/esquemas e a utilização de quaisquer dos instrumentos enumerados:

B1. Corrupção: Por favor, informe as incidências de corrupção relacionadas a este caso, se houver (suborno/tentativa de suborno de funcionários, terceiros, possível influência de pessoas politicamente expostas (PEPs) para influenciar funcionários de investigação ou funcionários de *Compliance* do setor privado nos bancos a serem subornados ou influenciados para permitir que produtos ilícitos do cibercrime sejam branqueados ou usados para fins de financiamento do terrorismo ou financiamento da proliferação

B3. Estratificação (smurfing): Numerosas transações envolvendo produtos ilícitos do cibercrime (depósitos, levantamentos, transferências) grandes volumes de pequenas transações e, por vezes, numerosas contas para evitar deteção e os limites que obrigam a comunicação

B4. Compra de mercadorias valiosas (pedras preciosas, metais preciosos, etc.): Utilização do produto da cibercriminalidade para adquirir instrumentos destinados a dissimular a verdadeira propriedade ou a movimentar valores sem serem detetados

B5. Compra de bens valiosos (terrenos/imóveis, veículos, etc.): Investimento dos produtos do cibercrime em bens negociáveis de elevado valor para encobrir a origem criminosa dos produtos.

B6. Branqueamento de capitais e financiamento do terrorismo com base no comércio: manipulação de faturas e utilização de rotas de financiamento do comércio e de mercadorias para o branqueamento dos produtos da cibercriminalidade

B7. Transferências eletrónicas: Transferência eletrónica de produtos ilícitos do cibercrime entre instituições financeiras de fora do país ou do país para outro país

B8. Investimento nos mercados de capitais: incidência da tentativa de encobrir a origem dos produtos da cibercriminalidade através do investimento no mercado de capitais e noutros instrumentos negociáveis

B9. Investimento empresarial: Mistura dos produtos do cibercrime com fundos comerciais legítimos, a fim de encobrir a origem dos fundos.

B10. Serviços alternativos de envio de dinheiro: Utilização de mecanismos informais de serviços monetários para transferir ou receber os produtos da cibercriminalidade

B11. Utilização de nomeados, fiduciárias, familiares ou terceiros, etc.: Transferência de produtos do cibercrime para nomeados, fiduciárias, familiares ou terceiros pelos traficantes de droga/criminosos organizados para proteger as suas identidades e/ou para guardar/ branquear.

B12. Utilização de APNFDs: Utilização de profissionais como contabilistas, agentes imobiliários, advogados, etc., para branquear os produtos do cibercrime

B13. Utilização de cartões de débito, cartões de crédito, outros cartões de pagamento, cheques, notas promissórias, etc.: Utilização de cartões, cheques, notas promissórias para receber/efetuar pagamentos ou branquear os produtos do cibercrime dentro da jurisdição nacional ou para outra jurisdição.

B14. Câmbios/conversão de numerário: Utilização do sistema de câmbio formal ou informal para branquear/transferir produtos do crime provenientes da cibercriminalidade

B15. Trocas de mercadorias (permuta): Troca direta de mercadorias (legais ou ilegais) para ocultar a origem do valor que são produtos de crimes do cibercrime

B16. Atividades de jogos (casinos, jogos de fortuna ou azar, etc.): Utilização de produtos do cibercrime para, por exemplo, comprar bilhetes premiados a jogadores legítimos, utilizar fichas de casino como moeda para transações criminosas, utilizar jogos de azar em linha para ocultar a origem dos produtos do crime.

B17. Uso abusivo de organizações sem fins lucrativos (OSFL): Utilização de organizações sem fins lucrativos para transferir produtos da infração doecibercrimes dentro do país ou para fora

B18. Uso de empresas/corporações de fachada: Incidências do uso de empresas de fachada para encobrir a identidade de pessoas envolvidas em crimes na indústria de ativos cibernéticos / virtuais

B19. Utilização de contas bancárias no estrangeiro: Movimentação dos produtos de cibercrimes de um ponto de elevada vigilância para um ponto de baixa vigilância (dentro ou fora do país)

B20. Fraude de identidade / identificação falsa: utilização de identidade falsa por pessoas envolvidas em casos de cibercrimes para ocultar a identificação dos envolvidos em muitos métodos de branqueamento de capitais (se possível, fornecer algumas informações sobre como obtiveram a falsa identidade – corrupção, intimidação, financiadores, etc.)

B21. Ativos Virtuais (VA) e Prestadores de Serviços de Ativos Virtuais (VASP): Utilização de produtos ilícitos provenientes da cibercriminalidade e de atividades de VA e utilização do ciberespaço e do espaço VA para branquear ou financiar o terrorismo ou a proliferação

B22. Financiamento do terrorismo: utilização dos produtos da cibercriminalidade para financiar ou facilitar o terrorismo e atividades terroristas (dentro ou fora do país)

B23. Queira apresentar um resumo do desfecho da investigação e/ou acusação judicial do caso
B24. Queira apresentar qualquer informação adicional sobre qualquer técnica/método não adequadamente coberto acima.

****



Complexe SICAP Point E,
Immeuble A, 1er Etage
Avenue Cheikh Anta Diop x Canal IV
B.P. : 32 400 Dakar - Ponty (Sénégal)
Standard : (+221) 33 859 18 18
Fax : (+221) 33 824 17 45
www.giaba.org