Humanity In War

MINUTA PARA A QUARTA CONSULTA COM OS ESTADOS

Linha de Trabalho 6 – RESPEITO AO DIREITO INTERNACIONAL HUMANITÁRIO (DIH) NO USO DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO DURANTE CONFLITOS ARMADOS

COPRESIDIDA POR Gana, Luxemburgo, México, Suíça e o Comitê Internacional da Cruz Vermelha.

Visão geral

As Tecnologias de Informação e Comunicação (TIC) se tornaram indispensáveis para a vida das pessoas em todo o mundo. Em nosso mundo digitalizado e conectado, serviços essenciais para a população civil, assim como a capacidade das pessoas de se conectarem com seus entes queridos e buscarem o desenvolvimento econômico, dependem da integridade e da disponibilidade de TIC. Em áreas afetadas por conflitos, TIC confiáveis são cruciais para que as pessoas civis acessem bens e serviços essenciais, para que os governos prestem serviços e para o apoio a serviços médicos e atividades humanitárias, incluindo as do Movimento Internacional da Cruz Vermelha e do Crescente Vermelho. Embora as capacidades das TIC possam permitir que os beligerantes alcancem objetivos militares sem necessariamente causar danos, ou com menos danos a civis ou bens civis do que as operações cinéticas, seu uso em conflitos contemporâneos também deu origem a atividades prejudiciais que afetam populações e infraestruturas civis, inclusive além das fronteiras internacionais.

A linha de trabalho destacou a necessidade imperiosa de proteger as populações civis e preservar a dignidade humana em conflitos atuais e futuros. Para tanto, é essencial defender e fortalecer o respeito

pelo Direito Internacional Humanitário (DIH) no uso das TIC durante conflitos armados, a fim de garantir que nossas infraestruturas, redes e capacidades de comunicação não sejam interrompidas, nossos dados não sejam apagados e nossas sociedades não sejam paralisadas.

A linha de trabalho também elaborou recomendações práticas, descritas abaixo, principalmente para

- proteger as populações, os dados e as infraestruturas civis contra atividades prejudiciais de TIC.
- salvaguardar os serviços médicos e as atividades humanitárias contra ameaças digitais e fazer cumprir as proibições de violência sexual e de recrutamento e utilização de crianças em hostilidades, inclusive por meios on-line.
- abordar a disseminação de informações em violação ao DIH.
- minimizar o risco de danos à população civil decorrentes do uso militar da infraestrutura civil de TIC e impedir que civis – de hackers a funcionários de empresas de tecnologia – envolvidos em atividades de TIC violem o DIH ou se coloquem inadvertidamente em risco.

Para promover o cumprimento do DIH em relação às atividades de TIC, a linha de trabalho destacou a importância de:

- reconhecer que, em áreas afetadas por conflitos, as TIC confiáveis são essenciais para civis, governos e atores humanitários, e que as atividades de TIC podem infligir custos humanos, incluindo sofrimento, ferimentos ou destruição, mesmo sem causar danos físicos, ressaltando a necessidade de defender a humanidade e a dignidade humana na guerra.
- comprometer-se a promover e esclarecer a aplicação do DIH às atividades de TIC e a adotar medidas práticas, de forma individual e coletiva, para mitigar os riscos à população civil e garantir que as atividades de TIC permaneçam consistentes com as proteções oferecidas pelo DIH.
- dar continuidade ao estudo e à discussão sobre como o DIH se aplica às atividades de TIC, com base nas discussões realizadas no âmbito desta linha de trabalho, com vistas a promover um entendimento comum que proteja pessoas civis contra danos.
- promover a transparência por meio do compartilhamento público de opiniões nacionais sobre como o direito internacional, incluindo o DIH, aplica-se às atividades de TIC, assim como o compartilhamento de lições aprendidas e boas práticas sobre a mitigação de danos a civis.
- apoiar o desenvolvimento de capacidades em âmbitos bilateral, regional e global para fortalecer a capacidade dos Estados de implementar e aplicar o DIH em relação às atividades de TIC.

Resultado

1. Proteger as populações, os dados e as infraestruturas civis contra danos decorrentes de atividades de TIC durante conflitos armados

Os conflitos armados contemporâneos mostram que as atividades de TIC podem representar riscos para a população civil, assim como para os dados e as infraestruturas civis. Tais atividades podem afetar gravemente civis e outras pessoas e bens protegidos, inclusive em casos de interrupção de serviços civis essenciais, como eletricidade, água, saneamento, telecomunicações, saúde, serviços humanitários e de emergência ou serviços financeiros, mesmo na ausência de danos físicos.

Na condução das atividades de TIC no contexto de um conflito armado e a ele associadas, é necessário cumprir o DIH em todos os momentos, incluindo os princípios da humanidade, da necessidade militar, da distinção, da proporcionalidade e da precaução.

As operações de TIC das quais se espera que possam causar morte ou ferimentos a pessoas, ou que resultem em danos ou destruição de bens, constituem ataques segundo o DIH. Isto inclui operações que possam desativar equipamentos ou sistemas e que exijam ações (como substituição, reinstalação ou reparação) para restaurar sua funcionalidade. Tais operações de TIC devem ser conduzidas em conformidade com todos os princípios e normas do DIH sobre a condução das hostilidades, incluindo as proibições de ataques contra civis e bens civis, ataques indiscriminados e ataques desproporcionais, e o princípio da precaução.

Os dados são essenciais em um mundo cada vez mais digitalizado e fundamentais para o funcionamento de serviços civis essenciais e atividades humanitárias. A forma como os dados são tratados durante conflitos armados pode afetar a vida e a dignidade das pessoas. Dados médicos, biométricos, financeiros e humanitários, entre outros, são parte integrante da prestação de serviços públicos e sociais. Apagar, manipular, negar o acesso ou divulgar esses dados sem autorização pode interromper serviços essenciais e expor pessoas e comunidades a sérios riscos.

Diversos princípios e normas do DIH oferecem proteção às populações, aos dados e às infraestruturas civis contra os perigos decorrentes das atividades de TIC durante conflitos armados, incluindo:

- o princípio de que uma parte em um conflito armado só pode recorrer aos meios e métodos de guerra necessários para enfraquecer as forças militares do inimigo.
- os princípios e normas que regem a condução das hostilidades, incluindo as proibições de ataques contra civis e bens civis, ataques indiscriminados e ataques desproporcionais, e o princípio da precaução.
- a obrigação de adotar medidas constantes para poupar a população civil, civis individualmente e bens civis na condução das operações militares.
- as normas que protegem a propriedade contra pilhagem, apreensão e destruição.

As atividades de coleta de informações em si não são proibidas pelo DIH, inclusive quando envolvem acesso a dados.

Para reforçar a proteção das populações, dos dados e das infraestruturas civis contra danos decorrentes de atividades de TIC durante conflitos armados, é essencial que os Estados e as partes em conflitos armados façam o seguinte:

a) Estabelecer e aplicar procedimentos rigorosos de seleção de alvos para operações de TIC a fim de garantir o cumprimento do DIH, incluindo a verificação de que os alvos se qualificam como objetivos militares e não estão sujeitos a proteção especial, e avaliar e prevenir, ou pelo menos minimizar, o risco de danos civis incidentais.

b) Basear as operações de TIC, incluindo os procedimentos de direcionamento, em todas as informações razoavelmente disponíveis, obtidas ativamente de fontes relevantes, incluindo dados e inteligência confiáveis, que sejam apoiadas por assessoria jurídica, conforme exigido pelo DIH; e, na medida do possível, buscar conhecimento especializado em segurança cibernética e outras áreas técnicas relevantes sobre a estrutura, interconectividade e dependências civis da infraestrutura de TIC.

c) Nos casos em que a infraestrutura de TIC constitua um objetivo militar segundo o DIH mas continue desempenhando funções civis, considerar todos os efeitos incidentais diretos e indiretos razoavelmente previsíveis sobre as populações, os dados e as infraestruturas civis,

resultantes da perda total ou parcial da sua utilização civil, incluindo o impacto nos serviços civis essenciais que prestam ou possibilitam, em conformidade com os princípios e normas de proporcionalidade e precaução no planeamento e na condução dos ataques.

d) Ao cumprir a obrigação de tomar todas as precauções viáveis na escolha dos meios e métodos de guerra, selecionar aqueles meios e métodos dos quais se espera que causem o mínimo de danos civis incidentais, inclusive avaliando rigorosamente se os meios e métodos habilitados por TIC ou outros meios e métodos não cinéticos reduziriam o risco de danos civis em comparação com as alternativas cinéticas disponíveis.

e) Aplicar limitações geográficas, temporais e sistêmicas apropriadas ("delimitações de zonas") na condução de operações de TIC, para evitar, ou pelo menos minimizar, o risco de danos incidentais a civis.

f) Monitorar de forma contínua as operações de TIC e garantir que haja capacidade para ajustá-las ou interrompê-las, a fim de evitar danos civis não intencionais ou excessivos. Sempre que possível, incorporar salvaguardas técnicas (como "interruptores de segurança" do tipo *kill-switches*) que permitam interromper, limitar ou isolar as operações de TIC caso haja risco de propagação para além do alvo pretendido, incluindo para redes ou infraestruturas civis ou de terceiros Estados.

2. Minimizar o risco de danos à população civil decorrentes do uso militar da infraestrutura civil de TIC durante conflitos armados

Com exceção de certas redes militares, o ambiente de TIC é predominantemente civil. No entanto, a interconexão entre redes civis e militares, e o uso militar da infraestrutura civil de TIC, criam desafios específicos para a sua proteção.

Nos casos em que a infraestrutura civil de TIC, incluindo a infraestrutura fornecida por empresas de tecnologia, é usada para fins militares, nem todo uso a torna (ou mesmo partes dela) um objetivo militar segundo o DIH. Contudo, o uso militar pode aumentar o risco de que essa infraestrutura seja atacada, expondo civis e bens civis fisicamente próximos, conectados digitalmente a ela ou dependentes dela a danos incidentais.

O DIH proíbe ataques a bens civis, incluindo infraestruturas civis de TIC. No entanto, o uso militar pode tornar essas infraestruturas, ou partes delas, objetivos militares.

Ao atacar tais objetivos militares, os Estados e as partes em conflito armado devem respeitar as proibições de ataques indiscriminados e desproporcionais e o princípio da precaução, inclusive nos casos em que a população civil depende dessa infraestrutura de TIC para o acesso a serviços essenciais. Sempre que possível, devem procurar realizar os ataques de forma a afetar apenas os componentes ou funções da infraestrutura de TIC usados para fins militares, e não aqueles que servem a funções civis.

Para proteger a população civil contra os efeitos dos ataques, os Estados e as partes em conflito armado devem, na medida do possível, tomar todas as precauções necessárias para proteger as pessoas civis e os bens civis sob seu controle contra os perigos decorrentes das operações militares.

A fim de minimizar o risco de danos à população civil decorrentes do uso militar da infraestrutura civil de TIC durante conflitos armados, e além das medidas estabelecidas no Resultado 1 acima, é essencial que os Estados e as partes em conflito sob cujo controle essa infraestrutura esteja localizada façam o seguinte:

a) Alocar recursos financeiros e técnicos adequados e adotar medidas de planejamento, projeto e configuração antes e durante conflitos armados.

b) Sempre que possível, separar física ou tecnicamente os componentes da infraestrutura de TIC usados para fins militares daqueles que servem a funções civis, inclusive por meio de segmentação de rede ou outras medidas de configuração apropriadas. Isto inclui, quando for viável, segregar os dados usados para fins militares daqueles que atendem a necessidades civis, por exemplo por meio de armazenamento e gestão separados e medidas de controle de acesso.

c) Fortalecer a resiliência da infraestrutura e dos serviços essenciais de TIC civis, inclusive por meio de redundância, planejamento de contingência e outras medidas para reduzir o risco de danos civis incidentais.

3. Minimizar os riscos relacionados à participação de civis em atividades de TIC durante conflitos armados no território de um Estado ou sob sua jurisdição ou controle

Nos conflitos armados atuais, a participação de civis em atividades de TIC durante os conflitos armados tornou-se mais acentuada. Em algumas situações, os Estados toleram, facilitam ou incentivam civis a realizarem atividades de TIC contra o adversário, incluindo atividades que podem afetar civis e bens civis.

À medida que se vê mais exposta às hostilidades, a população civil corre o risco de sofrer danos. Muitas pessoas podem desconhecer os riscos envolvidos, as potenciais consequências legais de sua conduta ou as normas do DIH que precisam seguir.

Civis – desde hackers a funcionários de empresas de tecnologia – devem cumprir o DIH ao realizar atividades de TIC no contexto de um conflito armado e a ele associadas.

Os Estados e as partes em conflitos armados são responsáveis pelas violações do DIH cometidas por civis, incluindo hackers e funcionários de empresas de tecnologia, cujas atividades de TIC durante o conflito armado lhes sejam atribuíveis. Os Estados devem exercer a devida diligência para prevenir que violações do DIH sejam cometidas ou facilitadas por atividades de TIC realizadas por civis em seu território ou sob sua jurisdição ou controle, e devem reprimir tais violações caso ocorram, em conformidade com suas obrigações segundo o DIH. Os Estados se comprometem a divulgar o DIH à população civil em seus respectivos países. Não devem encorajar, auxiliar ou ajudar civis a violarem o DIH, inclusive por meio de atividades de TIC.

Em certas circunstâncias específicas, a participação de civis em atividades de TIC pode equivaler à participação direta em hostilidades, o que significa que civis perdem a proteção contra os ataques, mas apenas durante o período em que seu envolvimento configurar participação direta. Em caso de dúvida, o DIH exige que uma pessoa seja considerada protegida contra os ataques.

Crianças não devem ser autorizadas a participar de hostilidades durante conflitos armados, incluindo por meio de atividades de TIC.

Para minimizar os riscos relacionados ao envolvimento de civis em atividades de TIC durante conflitos armados, é essencial que os Estados e as partes em conflito armado façam o seguinte:

a) Adotar medidas concretas para informar civis que possam estar envolvidos em atividades de TIC no contexto de um conflito armado sobre os riscos legais e práticos de fazer isso. Essas medidas podem incluir o compartilhamento de informações sobre as normas do DIH por meio de redes sociais, aplicativos específicos, rádio ou outros meios de comunicação de massa, ou o

desenvolvimento de códigos de conduta modelo que cumpram com o DIH e que os civis que realizam atividades de TIC devem ser solicitados a seguir.

b) Evitar, na medida do possível, o envolvimento de civis em operações de TIC que configurem participação direta em hostilidades, a fim de protegê-los dos perigos decorrentes de operações militares. Se, apesar disso, tal participação ocorrer, integrar civis às forças armadas na medida do possível.

c) Adotar todas as medidas viáveis para impedir que crianças participem em hostilidades através de atividades de TIC. Por exemplo, por meio de programas de educação e sensibilização para crianças e cuidadores; adaptando a legislação e as políticas nacionais para proibir o recrutamento e o uso de crianças para fins de combate on-line, e aplicando-as; e considerando restrições de idade ao acesso a ferramentas digitais que possam constituir participação direta em hostilidades, quando apropriado.

4. Proteger produtos e serviços de TIC civis fornecidos por empresas de tecnologia durante conflitos armados

Empresas de tecnologia fornecem cada vez mais serviços ou produtos de segurança cibernética e outras TIC a partes envolvidas em conflitos armados. Nessas situações, civis e bens civis que dependem desses produtos e serviços, ou a eles associados, podem ficar expostos a danos.

Ao mesmo tempo, os produtos e serviços de TIC fornecidos por empresas de tecnologia são amplamente utilizados pela população civil, por governos e por organizações humanitárias imparciais, inclusive durante conflitos armados. Sua interrupção, degradação ou uso indevido podem, portanto, ter consequências humanitárias significativas. Esses produtos e serviços de TIC para uso civil, assim como os funcionários civis que os fornecem, são protegidos pelo DIH.

Para reforçar a proteção de produtos e serviços de TIC civis fornecidos por empresas de tecnologia durante conflitos armados, essas empresas devem fazer o seguinte:

a) Ter em conta que o fornecimento de produtos e serviços de TIC às partes em conflito armado acarreta riscos tanto legais como práticos.

b) Compreender, avaliar e adotar medidas para minimizar os riscos de danos a civis e bens civis, sejam eles relacionados aos funcionários ou às propriedades dessas empresas, ou decorrentes de sua proximidade física, conexão digital ou dependência da infraestrutura ou dos respectivos serviços. Isso inclui, na medida do possível, separar física ou tecnicamente a infraestrutura, os serviços e os produtos utilizados para apoiar operações militares daqueles utilizados para fins civis.

c) Adotar medidas para impedir que seus funcionários se envolvam, facilitem ou se tornem cúmplices de violações do DIH, inclusive por meio do fornecimento de produtos ou serviços de TIC às partes em conflitos armados, e tomar as providências adequadas caso tais atos ocorram.

5. Salvaguardar os serviços médicos, as atividades humanitárias e outras pessoas, bens e atividades especificamente protegidos contra danos decorrentes de atividades de TIC durante conflitos armados

O setor de assistência à saúde e as organizações humanitárias imparciais são especialmente vulneráveis às atividades de TIC durante conflitos armados. A crescente dependência dos serviços médicos e humanitários por sistemas interligados e dados digitais significa que as interrupções na infraestrutura ou nos serviços de TIC podem afetar diretamente operações médicas que salvam vidas, comprometer dados sensíveis, prejudicar o trabalho de organizações humanitárias imparciais e seus funcionários, e colocar em risco a prestação de assistência essencial.

Equipes, unidades e veículos de saúde, assim como o pessoal e os bens humanitários, devem ser respeitados e protegidos em todos os momentos, em conformidade com o DIH, inclusive contra danos decorrentes de atividades de TIC. As atividades de TIC durante conflitos armados não devem interromper de forma indevida o funcionamento dos serviços médicos e das atividades humanitárias, incluindo os seus sistemas de dados, TIC e comunicação.

A confidencialidade dos dados médicos e humanitários deve ser respeitada, em conformidade com o DIH. Essa proteção é fundamental para preservar a confiança no trabalho dos serviços de saúde e das organizações humanitárias imparciais.

As partes em conflitos armados devem também adotar todas as medidas viáveis, nas circunstâncias em que estejam e em função dos recursos de que disponham, para evitar que os serviços médicos e as atividades humanitárias sejam prejudicados, inclusive por meio de atividades de TIC realizadas por terceiros, como criminosos cibernéticos e outros atores não estatais não atribuíveis a uma das partes em conflito.

Outros bens e atividades que gozam de proteção específica segundo o DIH, incluindo bens indispensáveis à sobrevivência da população civil, obras e instalações que contenham forças perigosas, bens culturais e de defesa civil, também podem enfrentar graves riscos decorrentes de atividades de TIC. A proteção específica que lhes é conferida deve ser respeitada, inclusive durante a realização de atividades de TIC em conflitos armados. Essa proteção inclui os seus dados e a infraestrutura de TIC indispensável ao seu funcionamento.

As atividades de TIC podem ser usadas para cometer ou facilitar atos de violência sexual ou para recrutar ou usar crianças em hostilidades. O DIH proíbe a violência sexual e o recrutamento e o uso de crianças em hostilidades, inclusive quando tais atos são cometidos por meio de atividades de TIC ou incentivados ou facilitados por elas.

Para salvaguardar os serviços médicos, as atividades humanitárias e outras pessoas, bens e atividades especificamente protegidos contra danos decorrentes de atividades de TIC durante conflitos armados, é essencial que os Estados e as partes em conflito armado façam o seguinte:

a) Apoiar discussões e esforços para tornar a proteção específica conferida pelo DIH aos serviços médicos e às atividades humanitárias identificável e visível no ambiente das TIC, inclusive por meio do desenvolvimento de um “emblema digital”, e continuar dialogando com o CICV sobre as vias jurídicas, técnicas e diplomáticas para sua implementação.

b) Reafirmar de forma explícita seu compromisso de respeitar e proteger os serviços médicos e as atividades humanitárias, incluindo os sistemas de dados, de TIC e de comunicação desses serviços e atividades, e de facilitar seu funcionamento no ambiente das TIC, assim como de respeitar a proteção específica dos bens indispensáveis à sobrevivência da população civil, incluindo seus dados e a infraestrutura de TIC indispensável ao seu funcionamento. Tais compromissos devem estar refletidos na legislação, nas políticas, na doutrina e na prática militar nacionais.

c) Sempre que possível, apoiar e facilitar o desenvolvimento de medidas adequadas de segurança cibernética e proteção de dados para prestadores de serviços médicos e organizações humanitárias imparciais, e auxiliar no fortalecimento de sua resiliência a ameaças de TIC que afetem seus sistemas e operações.

d) Reforçar os respectivos marcos legais e políticos nacionais que abordem a conduta on-line que possa constituir ou facilitar violações do DIH relacionadas com a violência sexual e com o recrutamento ou utilização de crianças em conflitos armados, e assegurar a implementação e a coordenação eficazes entre as respectivas autoridades.

e) Integrar salvaguardas específicas na doutrina militar, nos procedimentos operacionais padrão e nas regras de engajamento para prevenir e lidar com violações cometidas ou facilitadas por atividades de TIC, incluindo violência sexual e recrutamento ou uso de crianças em hostilidades. Medidas viáveis incluem regular o uso de dispositivos pessoais de TIC em contextos operacionais, restringir o compartilhamento de imagens ou informações sensíveis, proibir o uso de TIC para recrutar ou envolver crianças em hostilidades e educar crianças e responsáveis sobre os riscos associados.

6. Abordar a disseminação de informações em violação ao DIH

Nos conflitos armados contemporâneos, as atividades de TIC são cada vez mais utilizadas para disseminar informações que podem violar o DIH. Embora as operações de informação façam parte da guerra há muito tempo e não sejam ilegais em si mesmas, o uso das TIC, sobretudo por meio de plataformas de redes sociais ou aplicativos de mensagens, ou quando combinado com inteligência artificial e outras tecnologias emergentes, pode aumentar de forma significativa a velocidade, a escala e o alcance de informações prejudiciais.

Os Estados devem se abster de divulgar informações que violem o DIH, inclusive por meio do uso de TIC, e adotar todas as medidas viáveis para evitá-las. Isto inclui a disseminação de informações que incitem ou encorajem violações do DIH, exponham pessoas privadas de liberdade a insultos ou à curiosidade pública, ou cujo objetivo principal seja propagar o terror entre a população civil.

Os serviços médicos e as atividades humanitárias devem ser protegidos contra a desinformação facilitada pelas TIC cujo objetivo seja obstruir seu trabalho durante conflitos armados, já que tais atos interferem de forma indevida e são incompatíveis com a obrigação de respeitar e proteger o pessoal médico e humanitário e suas atividades.

Para combater a disseminação de informações em violação do DIH, é essencial que os Estados e as partes em conflito armado façam o seguinte:

a) Adotar todas as medidas viáveis para avaliar, prevenir e mitigar o risco de que operações de informação prejudiquem a população civil e outras pessoas protegidas, inclusive comprometendo sua segurança, dignidade ou acesso a serviços essenciais.

b) Abster-se de disseminar informações que desumanizem o adversário ou propaguem o ódio contra a população civil, inclusive por meio de TIC, e adotar as medidas apropriadas para garantir que suas forças armadas, outras autoridades públicas ou pessoas agindo em seu nome não se envolvam em tal conduta.

c) Apoiar, sempre que possível, os prestadores de serviços médicos e as organizações humanitárias imparciais no desenvolvimento de capacidades para reforçar a resiliência contra a desinformação e outras atividades de informação prejudiciais, inclusive facilitando sua

capacidade de reunir, verificar e divulgar informações precisas; reforçando sua preparação e planejamento de contingência para lidar com a exposição a informações prejudiciais; e incentivando o desenvolvimento de respostas adequadas a informações prejudiciais que afetem civis dentro de suas áreas de atuação.

d) Interceder junto a atores relevantes, incluindo o setor de tecnologia, para reduzir o risco de que plataformas on-line ou outros serviços de TIC sejam usados para incitar, incentivar ou facilitar violações do DIH ou prejudicar civis e bens civis. Isto pode incluir o desenvolvimento de marcos legais e de políticas adequados e a promoção, por parte de empresas de tecnologia, da adoção de salvaguardas e práticas destinadas a detectar, avaliar e lidar com informações prejudiciais em situações de conflito armado.

e) Fortalecer a resiliência da sociedade contra atividades relacionadas a informações prejudiciais, inclusive apoiando a disponibilidade de informações confiáveis, protegendo jornalistas e meios de comunicação quando exigido pelo DIH e outras normas aplicáveis e promovendo medidas de preparação que aumentem a capacidade da população civil de acessar informações confiáveis durante conflitos armados.

f) Abster-se de interromper o acesso da população civil à internet ou a outros serviços de TIC, considerando que tais medidas poderiam prejudicá-la. Caso as restrições sejam justificadas por imperiosa necessidade militar, adotar medidas de mitigação para minimizar ao máximo os efeitos adversos sobre as pessoas civis.

7. Medidas transversais para fortalecer a implementação do DIH em relação às atividades de TIC

É essencial que os Estados, ao cumprirem suas obrigações conforme o DIH em relação às atividades de TIC, façam o seguinte, inclusive por meio de medidas de implementação adotadas em tempos de paz:

a) Divulgar o conhecimento do DIH dentro das forças armadas e entre a população em geral, em particular entre as pessoas que possam estar envolvidas em atividades de TIC, e integrar os princípios e normas do DIH e sua aplicação às atividades de TIC na legislação nacional, na doutrina militar, nos procedimentos operacionais padrão e nas regras de engajamento e treinamento, conforme apropriado.

b) Disponibilizar assessores jurídicos qualificados para as unidades e comandos militares responsáveis pelas atividades de TIC, em particular no planejamento e na condução dessas operações.

c) Realizar análises jurídicas das capacidades das TIC que funcionam como novas armas, meios ou métodos de guerra, incluindo, entre outros, testes, avaliações, verificações e validações rigorosas das capacidades das TIC, para melhor compreender seu funcionamento, propagação e potenciais efeitos nos sistemas civis.

d) Adotar todas as medidas legislativas, regulatórias e de outra índole necessárias, incluindo, quando apropriado, sanções penais, para prevenir e reprimir violações do DIH cometidas por meio de atividades de TIC ou por elas facilitadas por pessoas ou em território sob sua jurisdição ou controle.

e) Adotar todas as medidas viáveis para prevenir ou limitar a proliferação, a reutilização ou o uso indevido de ferramentas e capacidades de TIC quando houver um risco evidente de que contribuam para violações do DIH.

f) Promover medidas voluntárias de compartilhamento de informações e fomento da confiança, com o objetivo de reduzir riscos para infraestruturas civis de TIC, incluindo o intercâmbio de boas práticas entre Estados, o estabelecimento de canais de comunicação e outras medidas práticas de redução de riscos e, quando apropriado, a comunicação voluntária de incidentes significativos de TIC que tenham causado danos não intencionais a civis, a fim de melhorar o entendimento coletivo e a mitigação de riscos.

g) Promover a transparência e o entendimento comum por meio do desenvolvimento e da divulgação pública de considerações nacionais sobre como o direito internacional, incluindo o DIH, aplica-se às atividades de TIC, e por meio do compartilhamento de lições aprendidas e boas práticas para minimizar danos os civis.

h) Apoiar o desenvolvimento de capacidades nos âmbitos bilateral, regional e global para reforçar a capacidade dos Estados de implementar e aplicar o DIH em relação às atividades das TIC.

i) Promover a cooperação entre Estados, empresas de tecnologia, organizações humanitárias imparciais e a sociedade civil para que utilizem as TIC de forma a reforçar a proteção de civis, inclusive por meio do desenvolvimento de orientações específicas para cada contexto ou de medidas práticas.

j) Incentivar a cooperação entre empresas de tecnologia e organizações humanitárias imparciais para melhorar a preparação e a resposta a ameaças de TIC que afetam pessoas e bens protegidos, inclusive por meio do compartilhamento de informações e do apoio à segurança cibernética, respeitando os princípios humanitários de neutralidade, imparcialidade e independência.

k) Integrar abordagens inclusivas, que levem em conta gênero, idade e deficiência, aos marcos nacionais e à prática operacional, a fim de fortalecer a implementação do DIH, inclusive na identificação e no enfrentamento dos riscos relacionados às TIC.

.