

# POLITICA DEL SETTORE DIFESA E SICUREZZA



---

# INDICE

<b>1. PREMESSA E FINALITÀ DEL DOCUMENTO</b>	<b>3</b>
<b>2. CONTESTO DI RIFERIMENTO</b>	<b>4</b>
2.1 CONTESTO REGOLAMENTARE E NORMATIVO ESTERNO	4
2.2 PRINCIPALE NORMATIVA INTERNA COLLEGATA	6
<b>3. PERIMETRO DI APPLICABILITÀ</b>	<b>7</b>
3.1 PERIMETRO PER TIPOLOGIA DI OPERAZIONE	7
3.2 PERIMETRO SOCIETARIO	7
<b>4. POSIZIONE DI CDP NEL SETTORE DELLA DIFESA E SICUREZZA</b>	<b>8</b>
4.1 CRITERI IN MATERIA DI OGGETTO DELL'OPERAZIONE	9
4.2 CRITERI IN MATERIA DI DESTINATARI FINALI	9
4.3 CRITERI IN MATERIA DI CONTROPARTI	10
4.4 CRITERI IN MATERIA DI PAESI DESTINATARI	11
<b>5. RUOLI E RESPONSABILITÀ</b>	<b>11</b>
<b>6. TRASPARENZA E RENDICONTAZIONE</b>	<b>13</b>
<b>7. ALLEGATI</b>	<b>13</b>
7.1 GLOSSARIO	13

# 1. PREMESSA E FINALITÀ DEL DOCUMENTO

Il Gruppo CDP promuove lo sviluppo del Paese, sia attraverso un ruolo di azionista stabile a presidio di infrastrutture e *asset* strategici, sia realizzando interventi di scopo per la crescita e l'internazionalizzazione delle imprese in settori chiave.

L'ampliamento progressivo del ruolo e dell'operatività di Cassa Depositi e Prestiti S.p.A. (di seguito "CDP"), riflesso anche nella modifica del 2021 allo Statuto<sup>1</sup>, rende necessaria l'adozione di indirizzi precisi, così come definiti all'interno del Piano Strategico, che prevedano l'integrazione sistematica degli aspetti ambientali, sociali e di *governance* lungo tutto il processo di Finanziamento/ Investimento in quanto considerati fattori imprescindibili per garantire lo sviluppo sostenibile e la generazione di maggiore valore sia per le imprese in cui investe che per la collettività.

CDP ritiene pertanto opportuno adottare indirizzi specifici in taluni settori rilevanti per il sistema Paese e che richiedono linee guida specifiche per l'allocazione delle risorse.

In particolare, il Settore della Difesa e Sicurezza rappresenta un settore strategico per garantire la sicurezza dei paesi ed è al contempo uno tra i settori più dibattuti in termini di compatibilità con i criteri di sostenibilità.

Il rapporto tra banche ed imprese coinvolte nella produzione e commercio di materiale di armamento è da tempo sotto gli occhi attenti di investitori, clienti, organizzazioni non governative e della società in senso più ampio. Con l'obiettivo ultimo di assicurare un contributo ai processi di pace, tali *stakeholder* intendono, infatti, evitare che finanziatori e aziende siano coinvolti in operazioni aventi ad oggetto le armi cosiddette "controverse", o con destinatario un paese oggetto di sanzioni internazionali o colpevoli di gravi abusi dei diritti umani e che si eviti di finanziare il terrorismo e il commercio illegale di armi. Inoltre, la limitata trasparenza impiegata dagli Stati nei processi di acquisto di armi per ragioni di sicurezza, aumenta l'attenzione che è necessario porre per evitare fenomeni di corruzione.

Nel corso degli ultimi anni, parallelamente alle iniziative intraprese da istituzioni internazionali volte a favorire il disarmo, la non proliferazione delle armi e l'istituzione di sistemi di controllo sul commercio delle armi, si è assistito ad un crescente dibattito sull'esigenza di rafforzare il supporto al settore della difesa, come conseguenza dei recenti sviluppi geopolitici e internazionali, a garanzia della sicurezza economica e la resilienza del sistema Paese.

I recenti sviluppi geopolitici e internazionali hanno inoltre evidenziato l'urgenza di garantire una maggiore protezione delle risorse fisiche e virtuali. La crescente esposizione di imprese, cittadini e istituzioni pubbliche a minacce informatiche ha infatti reso indispensabile rafforzare in modo coordinato le capacità di prevenzione, resilienza e protezione delle risorse strategiche, sia fisiche che digitali, garantendo una sicurezza efficace per cittadini, imprese e istituzioni pubbliche.

La difesa e la sicurezza consiste nell'insieme degli apparati destinati a tutelare l'integrità del territorio di uno Stato, la sicurezza della sua popolazione e il mantenimento delle sue istituzioni civili. In quest'ottica le linee strategiche e le scelte di produzione sono definite dallo Stato di riferimento che, per le aziende operanti in Italia, è lo Stato Italiano.

Alla luce del contesto e consapevole del proprio ruolo all'interno del Paese, nel 2022 CDP ha adottato una politica settoriale che disciplina il proprio approccio nel Settore della Difesa e Sicurezza al fine di assicurare il supporto ad un settore strategico per il Paese, garantendo al contempo la propria sostenibilità economico-finanziaria, di sostenibilità e reputazionale.

La presente Politica, coerentemente con le Politiche Generali di Finanziamento e Investimento Responsabile di CDP, si pone pertanto l'obiettivo di orientare l'operatività di CDP nel Settore della Difesa e Sicurezza stabilendo criteri di trattamento, di limitazione ed esclusione.

<sup>1</sup> Introduzione del principio di sviluppo sostenibile: "La società, nel perseguire la promozione della sostenibilità economica, sociale e ambientale nel lungo termine a beneficio degli azionisti e tenendo conto degli interessi degli altri *stakeholder* rilevanti per la società, ha per oggetto sociale..."

Il presente documento definisce:

- il contesto di riferimento (capitolo 2);
- il perimetro di applicabilità (capitolo 3);
- la posizione di CDP nel Settore della Difesa e Sicurezza (capitolo 4);
- i ruoli e le responsabilità dei soggetti coinvolti (capitolo 5);
- le modalità con cui viene garantita la trasparenza e la rendicontazione (capitolo 6).

Il presente documento è sottoposto a revisione periodica, anche al fine di riflettere, a titolo esemplificativo e non esaustivo, l'evoluzione normativa e regolamentare, il mutamento del contesto di riferimento e/o in caso di adozione di un nuovo piano strategico. Il riesame ha luogo, in ogni caso, ogni 3 anni.

La presente Politica, ove opportuno, va letta unitamente alle altre politiche, in particolare quelle Generali di Investimento e Finanziamento Responsabile, e alle fonti normative aziendali e/o di Gruppo pertinenti.

## 2. CONTESTO DI RIFERIMENTO

### 2.1 Contesto regolamentare e normativo esterno

Al momento dell'aggiornamento della presente Politica, il principale assetto regolatorio internazionale include i seguenti Trattati, Convenzioni e Regolamenti:

- Protocollo di Ginevra (1925), vieta l'uso in guerra di gas asfissianti, tossici o simili e di mezzi batteriologici;
- Trattato sulla messa al bando parziale degli esperimenti nucleari (*Partial Test Ban Treaty*, 1963), proibisce test nucleari le cui esplosioni provochino detriti radioattivi al di fuori dei limiti consentiti;
- Trattato di non-proliferazione nucleare (*Treaty on the Non-Proliferation of Nuclear Weapons*, 1970), rappresenta lo strumento di portata globale al fine di prevenire la diffusione delle armi nucleari e promuovere l'obiettivo del disarmo nucleare;
- Convenzione sulle armi biologiche (*Biological Weapons Convention*, 1975), vieta lo sviluppo, la produzione e la detenzione di armi batteriologiche (biologiche) e tossiniche (virus, batteri, microrganismi, spore, tossine) e impone la distruzione degli stock esistenti;
- ENMOD Convention (1978), convenzione che vieta l'uso di tecniche di modifica dell'ambiente a fini militari o ad ogni altro scopo ostile;
- Convenzione sul divieto o sulla limitazione dell'impiego di talune armi convenzionali (*Convention on Certain Conventional Weapons*, 1980) che possono essere ritenute capaci di causare effetti traumatici eccessivi o di colpire in modo indiscriminato;
- Accordo di Wassenaar (1996), promuove un regime di trasparenza e maggiore responsabilità nei trasferimenti di armi convenzionali e di beni e tecnologie a doppio uso. Con gli aggiornamenti del 2013 e 2015, questi presidi sono stati estesi anche a *software* e strumenti cibernetici, inclusi quelli destinati al cyber-spionaggio e agli attacchi informatici;
- Trattato sulla messa al bando totale degli esperimenti nucleari (*Comprehensive Nuclear-Test-Ban Treaty*, 1996), proibisce i test nucleari in qualsiasi ambiente, sia per scopi militari che pacifici;
- Trattato sulla messa al bando delle mine antipersona (Convenzione di Ottawa, 1997), vieta l'uso, la detenzione, la produzione e il trasferimento di mine antipersona e impone la distruzione degli stock esistenti nonché l'assistenza alle vittime del loro uso;
- Convenzione sulle armi chimiche (CAC, 1997), rappresenta il primo strumento internazionale sul disarmo delle armi chimiche e proibisce qualsiasi attività rivolta a sviluppo, produzione, acquisizione, detenzione, conservazione, trasferimento e uso di questa tipologia di armi e dei materiali ad esse collegati;
- Programma di azione delle Nazioni Unite per prevenire, combattere e sradicare il commercio illegale di armi leggere e di piccolo calibro (2001);
- Codice di condotta dell'Aia contro la proliferazione dei missili balistici (HCOC, 2002), regola l'area dei missili balistici in grado di trasportare armi di distruzione di massa e vuole istituire un regime di trasparenza e rafforzamento della fiducia sulla diffusione dei missili balistici. Gli Stati si impegnano volontariamente a fornire notifiche di pre-lancio sui lanci e sui voli di prova di missili balistici e veicoli di lancio spaziale;

- Convenzione di Budapest (ETS n. 185) del 2004, il primo trattato internazionale contro la criminalità informatica che definisce standard comuni e promuove la cooperazione tra Stati per contrastare reati digitali. Nel 2023 è stato adottato un Secondo Protocollo Aggiuntivo per migliorare la cooperazione internazionale, introducendo procedure accelerate per la condivisione di prove elettroniche e la collaborazione diretta con fornitori di servizi;
- Convenzione sul bando delle munizioni a grappolo (Convenzione di Oslo, 2008), vieta l'uso, la detenzione, la produzione e il trasferimento di munizioni a grappolo e impone la distruzione degli stock esistenti;
- Posizione Comune 2008/944/PESC del Consiglio dell'Unione Europea dell'8 dicembre 2008 (e successive modificazioni) che definisce norme comuni per il controllo delle esportazioni di tecnologia e attrezzature militari;
- Trattato sul commercio delle armi (*Arms Trade Treaty*, 2014), stabilisce dei criteri per l'autorizzazione (o proibizione) di trasferimenti di armi convenzionali;
- Trattato per la proibizione delle armi nucleari (2017), prevede l'impegno a non sviluppare, testare, produrre, acquisire, possedere, immagazzinare, usare o minacciare di usare armi nucleari;
- Trattato Globale ONU sulla Criminalità Informatica (adottato nel 2024 con entrata in vigore prevista dopo il 2026), accordo internazionale vincolante che rafforza la Convenzione di Budapest del 2001 e incoraggia la cooperazione internazionale nella prevenzione contro cybercrimini, affrontando reati come il terrorismo, la tratta di esseri umani, il traffico di droga e i crimini finanziari online;
- Regolamento (CE) N. 1236/2005 del Consiglio Europeo, relativo al commercio di determinate merci che potrebbero essere utilizzate per la pena di morte, per la tortura o per altri trattamenti o pene crudeli, inumani o degradanti;
- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 (*Cybersecurity Act*), che rafforza il mandato dell'ENISA, trasformandola in Agenzia dell'Unione europea per la cybersicurezza con compiti permanenti di coordinamento e supporto agli Stati membri, e istituisce un quadro europeo di certificazione della cybersicurezza per prodotti, servizi e processi ICT, finalizzato a garantire standard comuni, ridurre la frammentazione normativa e accrescere la fiducia nel mercato digitale europeo;
- Regolamento (UE) 2021/821 del Parlamento Europeo e del Consiglio che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso;
- Direttiva europea 2022/2555, nota come Direttiva *Network and Information Security* (di seguito "NIS2"), che istituisce un quadro giuridico unificato per garantire un elevato livello di sicurezza informatica nell'UE, estendendo l'applicazione a 18 settori critici, introducendo obblighi stringenti su gestione del rischio e notifica degli incidenti e rafforzando la responsabilità dei verticali aziendali;
- Regolamento (UE) 2025/38, noto come *Cyber Solidarity Act* (CSoA), in vigore dal 2025, integra la Direttiva NIS2 e introduce misure per rafforzare la capacità dell'UE di affrontare minacce informatiche, tra cui una rete di poli *cyber* europei e meccanismi di risposta agli incidenti *cyber*.

Anche l'Agenda 2030 dell'ONU intende contribuire all'instaurazione di sistemi nazionali di controllo degli armamenti solidi e trasparenti. Infatti, il raggiungimento di molti degli obiettivi individuati dall'Agenda dipende dalla riduzione della violenza armata e dall'aumento della sicurezza internazionale.

A livello nazionale, il principale riferimento normativo in termini di armamenti è costituito dalla Legge 185/90 e s.m.i. (e relativa normativa di attuazione) che disciplina il controllo dell'esportazione, importazione e transito dei materiali di armamento e prevede sanzioni amministrative pecuniarie in relazione alla violazione degli obblighi dalla stessa previsti.

Il quadro nazionale è integrato dalle seguenti disposizioni:

- Legge 9 dicembre 2021, n. 220, introduce da un lato il divieto di finanziamento, sotto qualsiasi forma, di società coinvolte in attività di costruzione, produzione, sviluppo, assemblaggio, riparazione, conservazione, impiego, utilizzo, immagazzinaggio, stoccaggio, detenzione, promozione, vendita, distribuzione, importazione, esportazione, trasferimento o trasporto di mine antipersona, munizioni e submunizioni cluster o di parti di esse; dall'altro lato il divieto di svolgimento (o di attività di supporto nello svolgimento) di attività di ricerca tecnologica, fabbricazione, vendita e cessione, a qualsiasi titolo, esportazione, importazione e detenzione di munizioni e submunizioni cluster o di parti di esse;
- Istruzioni di Banca d'Italia, COVIP, IVASS e MEF per contrastare il finanziamento delle imprese produttrici di mine antipersona, di munizioni e submunizioni a grappolo in attuazione dell'articolo 3, comma 1, della Legge 9 dicembre 2021, n. 220;
- Legge 18 aprile 1975, n. 110, disciplina il controllo delle armi, delle munizioni e degli esplosivi, definendo sia le armi da guerra che le armi comuni da sparo.

Allo stesso modo, in riferimento specifico alla sicurezza dei dati, il Governo ha sostenuto gli sforzi delle principali istituzioni nazionali e internazionali nel promuovere misure per la Cybersicurezza, adeguando il quadro normativo attraverso i seguenti provvedimenti:

- Decreto legge 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133, che istituisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC), definendo gli ambiti, i soggetti e le procedure per la protezione delle reti, dei sistemi informativi e dei servizi informatici di interesse nazionale, nonché i compiti di coordinamento e vigilanza attribuiti alla Presidenza del Consiglio e al Dipartimento delle Informazioni per la Sicurezza (DIS);
- Decreto legislativo 3 agosto 2022, n. 123, che disciplina il quadro di certificazione nazionale e aggiorna le norme italiane al Titolo III del Cybersecurity Act (Regolamento (UE) 2019/881), definendo i soggetti coinvolti, le procedure di rilascio e controllo delle certificazioni di Cybersicurezza, nonché i compiti dell’Agenzia per la Cybersicurezza Nazionale come autorità competente;
- Legge 21 giugno 2024, n. 90, che rafforza ulteriormente il sistema nazionale di Cybersicurezza introducendo misure per l’attuazione coordinata delle politiche di sicurezza digitale, potenziando le funzioni operative dell’Agenzia per la Cybersicurezza Nazionale e favorendo la cooperazione pubblico-privato nella protezione delle infrastrutture critiche, con successivi decreti attuativi (es. DPCM 30 aprile 2025) che ne definiscono l’organizzazione operativa e le modalità di coordinamento interistituzionale;
- Decreto legislativo 18 settembre 2024, n. 138, che recepisce la Direttiva UE 2022/2555 NIS2, rafforzando la Cybersicurezza di reti e sistemi informativi critici, nonché degli enti pubblici e privati operanti in settori essenziali (es. energia, sanità, trasporti, ecc.) e attribuendo all’Agenzia per la Cybersicurezza Nazionale compiti di coordinamento, vigilanza e supporto all’attuazione delle misure di sicurezza.

## 2.2 Principale normativa interna collegata

Le fonti normative aziendali, in aggiunta al presente documento, all’interno delle quali CDP sancisce e riconosce i principi di sostenibilità quali valori fondanti sono, a titolo esemplificativo e non esaustivo:

- Statuto;
- Codice Etico;
- Modello di Organizzazione Gestione e Controllo ex D. Lgs. 231/2001;
- Framework di Sostenibilità;
- Politica Generale di Finanziamento Responsabile;
- Politica Generale di Investimento Responsabile;
- Politica del Settore Energia;
- Politica del Settore Trasporti di CDP;
- Politica del Settore Agricolo, dell’Industria Alimentare, del Legno e della Carta;
- Politica Generale di Stakeholder Engagement;
- Politica Generale Stakeholder Grievance Mechanism;
- Politica Generale di Diversità, equità e inclusione;
- Politica Generale Rischi;
- Regolamento del Credito.

Il presente documento va letto unitamente alle politiche generali, in particolar modo a quelle di Finanziamento e Investimento Responsabile.

Il quadro regolatorio e normativo di riferimento è completato da ulteriori fonti normative interne ove sono declinati i principi, le metodologie e le modalità operative attraverso cui la sostenibilità viene perseguita all’interno dell’organizzazione aziendale o per l’operatività specifica nel Settore della Difesa e Sicurezza, quali ad esempio l’Istruzione operativa di Gruppo “Adempimenti normativi e operativi del settore Difesa e Sicurezza”.

## 3. PERIMETRO DI APPLICABILITÀ

### 3.1 Perimetro per tipologia di operazione

Il perimetro di applicabilità del presente documento è riferibile all'operatività di CDP nel Settore della Difesa e Sicurezza, relativamente alle operazioni originate dopo l'approvazione del presente documento<sup>2</sup>, sia di Investimento (in modalità diretta e, laddove possibile, in modalità indiretta) sia di Finanziamento (nella sola modalità diretta<sup>3</sup>), e rinnovo di tali operazioni. La Politica non si applica alle operazioni<sup>4</sup> su partecipazioni già detenute in portafoglio e alle modifiche contrattuali di Finanziamento. Per gli investimenti in portafoglio, in coerenza con quanto presente nella Politica Generale di Investimento Responsabile, a cui si rimanda, CDP effettua un monitoraggio attivo e, allo stesso tempo, collabora con il management delle società, al fine di discutere possibili linee guida per i piani di sviluppo e per effettuare specifici approfondimenti su tematiche ad hoc. L'attività di *engagement*, svolta regolarmente, consente inoltre di ravvisare eventuali problematiche emergenti in fase di gestione dell'investimento e concordare le azioni necessarie da implementare che saranno verificate attraverso un apposito monitoraggio.

Si precisa che nell'ambito della sua *mission* istituzionale, CDP è chiamata anche a gestire, per effetto di specifiche disposizioni normative, e/o appositi mandati, fondi di terze parti (es. risorse dei Ministeri). L'attività relativa a tale ambito è svolta nel rispetto dei vincoli normativi vigenti e degli indirizzi delle Istituzioni interessate.

In aggiunta, e al fine di rendere più stringenti i criteri di operatività nel settore, sono incluse anche le operazioni immobiliari che hanno ad oggetto la locazione e/o la cessione di immobili nei confronti di Controparti attive nel Settore della Difesa e Sicurezza secondo quanto previsto dal paragrafo 4.3 "Criteri in materia di Controparti".

Si precisa inoltre che i criteri di esclusione in materia di Controparti si applicano a tutte le operazioni indipendentemente dal settore.

Una operazione si intende riferita al Settore della Difesa e Sicurezza nei seguenti casi:

- i. Operazione di Finanziamento/Investimento con scopo generico, qualora le Controparti abbiano avuto un fatturato derivante dal Settore della Difesa e Sicurezza pari ad almeno il 20% nel corso dell'ultimo triennio;
- ii. Operazione di Finanziamento/Investimento con scopo specifico che abbia quale oggetto principale beni riconducibili a tale Settore.

Considerando la particolare attenzione di CDP agli aspetti reputazionali connessi alle operazioni di esportazione concernenti il Settore della Difesa e Sicurezza, si statuisce che la delibera di tali operazioni è rimessa alla competenza esclusiva del Consiglio di Amministrazione di CDP, su proposta dell'Amministratore Delegato, previo parere obbligatorio non vincolante del Comitato Rischi e Sostenibilità.

Il Consiglio di Amministrazione di CDP può, inoltre, caso per caso, anche sulla base dell'istruttoria svolta dalle strutture competenti, approvare eventuali deroghe o interventi in deroga al presente documento, nel rispetto della normativa interna vigente, e in particolare di quanto stabilito rispettivamente nella Politica Generale di Finanziamento Responsabile e nella Politica Generale di Investimento Responsabile.

### 3.2 Perimetro Societario

La presente Politica si applica, con le specifiche di cui sopra, alle operazioni svolte da CDP S.p.A. nel Settore della Difesa e Sicurezza.

CDP si impegna affinché le Società soggette a direzione e coordinamento<sup>5</sup> di CDP che hanno adottato una politica nel Settore della Difesa e Sicurezza coerente con la Politica di CDP<sup>6</sup> recepiscono gli aggiornamenti di volta in volta apportati alla presente Politica, nel rispetto del principio di proporzionalità e tenuto conto dei profili di autonomia decisionale posta in capo agli Organi Societari delle Società del Gruppo ed in particolare dei Soggetti vigilati<sup>7</sup>, nonché della specifica normativa di settore a cui quest'ultimi sono sottoposti.

<sup>2</sup> Le modifiche introdotte con questo aggiornamento saranno applicabili alle operazioni originate a partire dalla data di approvazione della presente Politica.

<sup>3</sup> Sono pertanto esclusi tutti i finanziamenti in modalità indiretta.

Si precisa che i presidi previsti dalla legge 220/2021 e relative Istruzioni Attuative sono applicati a tutte le operazioni, anche indirette e/o con risorse di terzi, rientranti nel perimetro di applicazione di tale norma dettagliato all'interno di apposita normativa interna, e comunque, nel rispetto della normativa esterna applicabile alla specifica operatività.

<sup>4</sup> Include operazioni *equity* e similari (e.g. acquisto, scissioni, fusioni, conversioni di azioni, trasformazioni, concessioni di finanziamenti soci o versamenti in conto capitale, sottoscrizione strumenti ibridi, sottoscrizione convertibili, aumenti di capitale, salvo che questi ultimi riguardino l'acquisto di una società che opera nel settore).

<sup>5</sup> Ai sensi degli articoli 2497 e seguenti del Codice civile.

<sup>6</sup> SIMEST S.p.A., CDP Equity S.p.A..

<sup>7</sup> Società sottoposte ad un regime autorizzativo, regolamentare, ispettivo e informativo da parte delle Autorità di Vigilanza di settore (e.g., Banca d'Italia e IVASS).

## 4. POSIZIONE DI CDP NEL SETTORE DELLA DIFESA E SICUREZZA

CDP, nel rispetto del contesto normativo e statutario di riferimento, orienta il proprio approccio strategico ed operativo indirizzando l'utilizzo di risorse verso ambiti prioritari così come identificati nel Piano Strategico. Con specifico riferimento al settore trattato dal presente documento, il Piano di CDP 2025-2027 ha identificato la Sicurezza Economica e l'Autonomia strategica come uno tra i macro-obiettivi di interesse strategico, definendo la Sicurezza e Difesa come ulteriore campo di intervento per l'azione di CDP, ad integrazione dei 10 già definiti nel Piano 2022-24. CDP intende operare nel Settore della Difesa e Sicurezza al fine di: i) rafforzare la capacità produttiva del Paese negli ambiti strategici, riducendo le dipendenze da fattori produttivi e input critici; ii) contribuire allo sviluppo e alla protezione di infrastrutture critiche, soprattutto in ambito energetico e digitale; iii) accrescere la proiezione internazionale del Paese, consolidando relazioni economiche paritarie in un'ottica strategica e rafforzando l'impegno nella cooperazione internazionale; iv) rispondere alle esigenze di difesa e sicurezza degli Stati, anche contribuendo a garantire processi di pace.

Allo stesso tempo, CDP ritiene sia di primaria importanza che le Controparti e i paesi coinvolti nelle operazioni abbiano adeguati presidi in grado di assicurare che i beni oggetto della Politica siano utilizzati esclusivamente nel rispetto dei diritti umani e dei principi definiti dalle convenzioni internazionali. Pertanto, CDP valuta la capacità delle Controparti e dei paesi di garantire che tali beni non siano utilizzati per scopi differenti da quelli previsti dalla presente Politica come, a titolo esemplificativo e non esaustivo, l'utilizzo da parte di organizzazioni terroristiche o altri gruppi armati, l'utilizzo contro la popolazione civile in violazione dei diritti umani, nonché l'utilizzo di strumenti tecnologici per finalità illecite che possano comportare usi impropri, accessi non autorizzati o compromissioni digitali dei beni e delle informazioni ad essi connesse.

L'operatività di CDP nel Settore della Difesa e Sicurezza è svolta nel pieno rispetto delle principali Convenzioni e Trattati Internazionali in materia di armi e di Cybersicurezza, delle disposizioni normative emanate a livello europeo e della legislazione italiana. In riferimento a quest'ultima, CDP assicura il rispetto delle disposizioni e degli obblighi informativi previsti dalla legge 185/1990, del Decreto Legislativo 109/2007 (ripreso anche dal D.Lgs 231/07) e dalla legge 220/2021 e relative Istruzioni Attuative. Pertanto, le disposizioni previste all'interno del presente documento sono da intendersi come aggiuntive e non sostitutive rispetto a quanto previsto da tali normative.

Alla luce dei suddetti principi, CDP ha definito alcuni criteri per indirizzare le proprie attività all'interno del Settore della Difesa e Sicurezza. Tali criteri, dettagliati nei paragrafi seguenti, riguardano:

- la tipologia di beni per la difesa e sicurezza oggetto dell'operazione;
- il destinatario finale dell'operazione;
- la Controparte dell'operazione;
- il paese destinatario dei beni oggetto dell'operazione.

Si precisa che nell'ambito dell'attività svolta da CDP in ambito cooperazione internazionale, oltre ai criteri di esclusioni indicati nei paragrafi seguenti, si applicano le esclusioni derivanti dalla partecipazione di CDP a *European Development Finance Institution* (EDFI)<sup>9</sup>.

Per le operazioni nel Settore della Difesa e Sicurezza CDP, oltre ad aver identificato delle casistiche di esclusione dell'operatività, ha definito uno specifico modello di valutazione dell'operazione in riferimento alle Controparti e ai paesi di destinazione dei beni oggetto dell'operazione. Qualora dall'analisi effettuata emergano delle criticità, l'esito della valutazione contiene la proposta di procedere con delle limitazioni a seconda del livello di criticità riscontrato.

<sup>8</sup> Il D.Lgs109/07 definisce il finanziamento della proliferazione di armi di distruzione di massa come: «La fornitura o la raccolta di fondi e risorse economiche, in qualunque modo realizzata e strumentale, direttamente o indirettamente, a sostenere o favorire tutte quelle attività legate all'ideazione o alla realizzazione di programmi volti a sviluppare strumenti bellici di natura nucleare, chimica o batteriologica». CDP, in linea con la *Policy* Antiriciclaggio e la *Policy* Sanzioni Finanziarie Internazionali, prevede specifici controlli rafforzati per valutare attentamente il rischio che un cliente o una transazione possa essere collegata alla proliferazione e analizzare elementi quali la trasparenza dell'assetto proprietario, lo scopo dell'operazione, coinvolgimento di paesi a rischio, coerenza economica dell'operazione, acquisti di beni o tecnologie sensibili.

<sup>9</sup> Harmonized EDFI Exclusion List: [https://edfi.eu/wp-content/uploads/2024/10/EDFI-Exclusion-List\\_September-2011.pdf](https://edfi.eu/wp-content/uploads/2024/10/EDFI-Exclusion-List_September-2011.pdf)

Ai fini dell'applicazione della presente Politica, CDP acquisisce dalla Controparte, con le modalità definite nelle Politiche Generali di Finanziamento e Investimento Responsabile, e declinate nella normativa interna di dettaglio, la documentazione necessaria a condurre le valutazioni<sup>10</sup>.

In alcune specifiche circostanze, qualora ritenuto necessario, CDP può avvalersi del contributo consulenziale da parte di esperti indipendenti per supporto nella valutazione circa il rispetto dei requisiti identificati dalla Politica.

## 4.1 Criteri in materia di oggetto dell'operazione

CDP non intende supportare in alcun modo beni che abbiano effetti indiscriminati e possano causare indebitamente danni e lesioni gravi, quali a titolo esemplificativo le armi controverse e/o per la tortura.

Pertanto, per le Operazione di Finanziamento/Investimento con scopo specifico, CDP si astiene dal partecipare a qualsiasi titolo a operazioni che abbiano ad oggetto:

- armi controverse<sup>11</sup> e/o loro componenti chiave<sup>12</sup> quali:
  - armi nucleari;
  - armi chimiche;
  - armi biologiche;
  - armi all'uranio impoverito;
  - mine anti-persona;
  - mine anti-carro;
  - munizioni e submunizioni cluster / bombe o munizioni a grappolo;
- armi comuni da sparo, armi leggere e di piccolo calibro, a meno che (i) abbiano come destinatario finale esclusivo le forze armate e/o di Polizia<sup>13</sup> o (ii) riguardino armi prodotte/commercializzate esclusivamente per uso sportivo, o (iii) riguardino armi commercializzate nei paesi dell'UE;
- merci utilizzabili solo per la pena di morte, per la tortura o per altri trattamenti o pene crudeli, inumani o degradanti<sup>14</sup>;
- le seguenti armi cibernetiche: strumenti digitali o *software* malevoli (es. *malware*, *ransomware*)<sup>15</sup> progettati appositamente per essere utilizzati o destinati a causare danni, distruzione o compromissioni a sistemi informatici, infrastrutture critiche, reti o dati a meno che tali beni (i) abbiano come destinatario finale esclusivo le forze armate, di Polizia e/o i governi<sup>16</sup>, o (ii) siano finalizzati al miglioramento della robustezza dei sistemi aziendali e/o di pubblica utilità.

Le operazioni relative ai materiali di armamento e ai beni a duplice uso che risultano ammissibili sono soggette alla verifica del rispetto degli ulteriori criteri di seguito elencati.

## 4.2 Criteri in materia di destinatari finali

CDP intende operare nel settore con l'obiettivo di rispondere alle esigenze di difesa e sicurezza dei paesi ed intende escludere operazioni che abbiano come destinatari finali privati cittadini o altre organizzazioni che possano utilizzare i beni oggetto della Politica per altri scopi, come ad esempio il terrorismo o l'impiego illecito delle informazioni e dei dati acquisiti, anche tramite attacchi informatici o violazioni dei sistemi digitali.

Pertanto, per le Operazione di Finanziamento/Investimento con scopo specifico CDP ritiene ammissibili esclusivamente le operazioni che abbiano come unico destinatario finale un governo o un'impresa da esso autorizzata e che siano conformi a quanto stabilito dalla legge 185/1990.

<sup>10</sup> Nelle proprie attività di valutazione, in linea con quanto previsto dalla *Policy* di Gruppo Sanzioni Finanziarie Internazionali, CDP si conforma alle misure ivi individuate.

<sup>11</sup> Per una definizione estensiva delle armi controverse e della relativa legislazione collegata si rimanda al glossario.

<sup>12</sup> Componente critico necessario per il funzionamento dell'arma controversa e appositamente progettato a tale scopo.

<sup>13</sup> Il paese di riferimento è oggetto di analisi come rappresentato al paragrafo 4.4 "Criteri in materia di paesi destinatari" nel quale sono descritti i relativi criteri di esclusione e valutazione.

<sup>14</sup> Beni di cui al Regolamento (UE) 2019/125.

<sup>15</sup> Per una definizione estensiva delle principali tipologie di *software* malevoli progettati per attacchi informatici si rimanda al glossario.

<sup>16</sup> Il paese di riferimento è oggetto di analisi come rappresentato al paragrafo 4.4 "Criteri in materia di paesi destinatari" nel quale sono descritti i relativi criteri di esclusione e valutazione.

## 4.3 Criteri in materia di Controparti<sup>17</sup>

CDP intende instaurare rapporti solo con Controparti che rispettino la legislazione vigente, le restrizioni internazionali in materia di armi, nonché le convenzioni internazionali ratificate dal nostro Paese.

Oltre al rispetto delle prescrizioni normative, CDP intende definire ulteriori criteri che devono essere rispettati dalle Controparti.

CDP, pertanto si astiene dal partecipare a qualsiasi titolo ad operazioni che abbiano come Controparte un'azienda che:

- direttamente o indirettamente<sup>18</sup> attraverso società controllate/collegate o controllanti, svolge attività di produzione, commercio, stoccaggio, vendita, cessione, importazione, esportazione di armi controverse<sup>19</sup> e/o suoi componenti chiave<sup>20</sup> o svolge qualsiasi servizio associato a tali armi, ivi inclusa la ricerca tecnologica;
- produce e/o commercializza armi comuni da sparo, armi leggere e di piccolo calibro, a meno che l'operazione: (i) abbia come destinatario finale esclusivo le forze armate e/o di Polizia, o (ii) sia rivolta esclusivamente a finalità di R&S e di miglioramento dell'impatto ambientale/sociale dei processi aziendali, o (iii) riguardi armi prodotte/commercializzate esclusivamente per uso sportivo, o (iv) riguardi armi commercializzate nei Paesi dell'UE;
- produce e/o commercializza merci utilizzabili solo per la pena di morte, per la tortura o per altri trattamenti o pene crudeli, inumani o degradanti<sup>21</sup>;
- è vietata ex L. 220/2021<sup>22</sup>;
- produce e/o commercializza armi cibernetiche: strumenti digitali o *software* malevoli (es. *malware*, *ransomware*)<sup>23</sup> progettati appositamente per essere utilizzati o destinati a causare danni, distruzione o compromissioni a sistemi informatici, infrastrutture critiche, reti o dati, a meno che tali beni (i) abbiano come destinatario finale esclusivo i governi, le forze armate e/o di Polizia, o (ii) siano finalizzati al miglioramento della robustezza dei sistemi aziendali e/o di pubblica utilità.

Fermo restando i criteri di esclusione sopra esplicitati, CDP valuta le Controparti operanti nel Settore della Difesa e Sicurezza in base all'approccio di gestione dei temi di sostenibilità materiali per il settore, alla *governance*, incluse le procedure adottate per operare in paesi che ledono i diritti umani e/o con alto indice di corruzione in linea con quanto previsto dalla presente Politica e per gestire il rischio di corruzione delle attività aziendali, e al loro coinvolgimento in controversie ESG.

Laddove ad esito delle valutazioni e verifiche effettuate dovessero emergere delle carenze, CDP svolge un'attività di *engagement* con la Controparte al fine di individuare eventuali misure correttive o di gestione delle criticità riscontrate, integrando le risultanze emerse dal confronto nel proprio processo valutativo. Nel caso in cui dalle analisi complessive emergano criticità particolarmente rilevanti e in assenza di *mitigant*, CDP può valutare di procedere nell'operazione con limitazioni crescenti.

Nel caso di operazioni di Finanziamento/Investimento con scopo specifico, tali valutazioni sulla Controparte, insieme alle valutazioni su paesi destinatari, contribuiscono alle valutazioni complessive dell'operazione.

<sup>17</sup> Per Operazioni di esportazione le valutazioni riguardano le società esportatrici e, ove rilevante e possibile, le altre aziende coinvolte nell'operazione.

<sup>18</sup> Si intendono indirettamente coinvolte: a) società controllate/collegate ex art. 2359 c.c. da società o entità implicate nella produzione, commercio, stoccaggio o ogni altra attività o servizio associato con le "armi controverse" o di componenti chiave di uno dei sistemi delle predette armi, anche se queste società non operano nel settore delle armi; b) Società controllanti dirette di società o entità implicate nella produzione, commercio, stoccaggio o ogni altra attività o servizio associato con le "armi controverse" sopra specificate o di componenti chiave di uno dei sistemi delle predette armi, anche se queste società non operano nel settore delle armi.

Tali verifiche sono effettuate sulla base delle migliori informazioni disponibili.

<sup>19</sup> Armi nucleari (salvo i casi consentiti dai Trattati internazionali vigenti ratificati dal nostro Paese e in conformità agli obblighi derivanti dall'adesione alla NATO), armi chimiche, armi biologiche, armi all'uranio impoverito, mine antipersona, mine anti-carro, munizioni e submunizioni cluster/bombe o munizioni a grappolo.

<sup>20</sup> Componente critico necessario per il funzionamento dell'arma controversa e appositamente progettato a tale scopo.

<sup>21</sup> Beni di cui al Regolamento (UE) 2019/125.

<sup>22</sup> Si precisa che i presidi previsti dalla legge 220/2021 e relative Istruzioni Attuative sono applicati a tutte le operazioni, anche indirette e/o con risorse di terzi, rientranti nel perimetro di applicazione di tale norma dettagliato all'interno di apposita normativa interna e, comunque, nel rispetto della normativa esterna applicabile alla specifica operatività.

Per le operazioni rientranti nel perimetro della legge 220/2021, ed ai fini dei relativi divieti ivi espressi, il termine Finanziamenti deve essere inteso secondo la più ampia accezione e ricomprendere, conseguentemente, ogni forma di supporto finanziario effettuato anche attraverso società controllate, aventi sede in Italia o all'estero, tra cui, a titolo esemplificativo e non esaustivo, la concessione di credito sotto qualsiasi forma, il rilascio di garanzie finanziarie, l'assunzione di partecipazioni, l'acquisto o la sottoscrizione di strumenti finanziari.

<sup>23</sup> Per una definizione estensiva si rimanda al glossario.

## 4.4 Criteri in materia di paesi destinatari

Nell'ambito delle operazioni svolte nel Settore della Difesa e Sicurezza, CDP intende evitare qualsiasi complicità con le violazioni dei diritti umani nei conflitti armati e limitare il rischio di esportazioni verso paesi ove è in corso un conflitto armato, che non forniscano adeguate garanzie sull'effettivo utilizzo e destinazione finale delle armi, che siano esposti ad elevati rischi di corruzione.

A tal fine, per le Operazione di Finanziamento/Investimento con scopo specifico CDP<sup>24</sup> si astiene dal partecipare a qualsiasi titolo ad operazioni che coinvolgono paesi che

- sono soggetti ad embargo delle forniture belliche da parte dell'Unione Europea, dell'ONU o dell'OSCE; e/o
- versano in stato di conflitto armato, identificando tali paesi anche sulla base degli orientamenti di organismi italiani e internazionali.

Laddove il paese non rientri nelle categorie sopra elencate, CDP ne valuta:

- il livello di corruzione;
- il rispetto dei diritti umani;
- la presenza di controversie relative al settore;
- la ratifica dei principali trattati internazionali in materia di armi.

Le valutazioni sui paesi sulla base dei parametri sopra elencati vengono combinate con le valutazioni sulle Controparti descritte nel paragrafo 4.3 (tra cui l'analisi delle politiche adottate per valutare il rischio di violazioni dei diritti umani nei paesi in cui opera e prevenire i rischi di corruzione) per identificare la valutazione complessiva dell'operazione. Nel caso in cui l'operatività in un paese attenzionato si combini con politiche della controparte ritenute non del tutto soddisfacenti, CDP adotta delle limitazioni crescenti alla sua partecipazione nell'operazione, in funzione della criticità riscontrata.

## 5. RUOLI E RESPONSABILITÀ

Alla luce del contesto delineato, si definiscono di seguito i ruoli e le responsabilità - nel rispetto ed in conformità del sistema normativo, organizzativo e dei poteri e delle deleghe interne aziendali - dei diversi soggetti coinvolti.

### **Consiglio di Amministrazione**

- approva in via esclusiva e non delegabile il presente documento nonché ogni sua revisione di carattere non formale e la relativa eventuale abrogazione;
- delibera in via esclusiva, su proposta dell'Amministratore Delegato, previo parere obbligatorio non vincolante del Comitato Rischi e Sostenibilità, tutte le operazioni di esportazione inerenti il Settore della Difesa e Sicurezza;
- valuta se è opportuno intervenire nelle operazioni di Finanziamento/Investimento anche negli ambiti esclusi dal presente documento, approvando eventuali deroghe o interventi in deroga, secondo quanto indicato al capitolo 3 "Perimetro di Applicabilità".

### **Comitato Rischi e Sostenibilità**

- rilascia parere al Consiglio di Amministrazione sul presente documento nonché sulle sue revisioni;
- rilascia parere obbligatorio e non vincolante sulle operazioni concernenti il Settore della Difesa e Sicurezza nell'ambito delle proprie competenze;
- rilascia pareri specifici su eventuali deroghe.

<sup>24</sup> In linea con quanto previsto dalla Policy di Gruppo Sanzioni Finanziarie internazionali, CDP si conforma alle misure restrittive di natura oggettiva ivi individuate, così come sinteticamente riportate all'interno delle singole Schede Paese allegate alla Policy di Gruppo Sanzioni Finanziarie internazionali.

### **Amministratore Delegato**

- propone al Consiglio di Amministrazione l'approvazione della presente Politica, nonché eventuali modifiche;
- supervisiona nel continuo, ricevendo a tal fine flussi informativi, l'applicazione di quanto stabilito dalla presente Politica, garantendo un assetto organizzativo funzionale all'obiettivo.

### **Direzione Amministrazione, Finanza, Controllo e Sostenibilità**

- assicura la definizione di proposte di aggiornamento del presente documento, nel rispetto delle Linee Guida Strategiche di volta in volta definite, anche sulla base delle tematiche rilevanti identificate, in coordinamento con le altre strutture competenti, in coerenza con quanto definito nell'Istruzione operativa di Gruppo "Adempimenti normativi e operativi del settore Difesa e Sicurezza", garantendo un supporto consulenziale nel continuo in merito alla relativa interpretazione;
- garantisce, in collaborazione con le strutture coinvolte, la corretta implementazione della presente Politica, valutando la coerenza delle diverse linee d'intervento di CDP con i principi ivi definiti, contribuendo, congiuntamente alle strutture interessate, alle necessarie integrazioni del *framework* contrattuale;
- assicura le analisi necessarie al rispetto dei criteri di cui alla presente Politica, al fine di definire un giudizio di sintesi finale circa l'ammissibilità dell'operazione;
- presidia il dialogo con le agenzie di *rating* ESG al fine di acquisire informazioni e contenuti volti a contribuire al miglioramento del presente documento.

### **Direzione Pubblica Amministrazione**

- contribuisce in coordinamento con la Direzione Amministrazione, Finanza, Controllo e Sostenibilità all'aggiornamento della presente Politica, per quanto riguarda la *Cybersecurity*;
- garantisce, in collaborazione con le strutture coinvolte, la corretta implementazione della presente Politica per quanto attiene gli ambiti di *Cybersecurity*.

### **Direzione Strategie Settoriali e Impatto**

- assicura la definizione e l'aggiornamento delle Linee Guida Strategiche funzionali ad indirizzare le priorità di intervento volte a colmare i *gap* di mercato/ socioeconomici;
- assicura, nell'ambito della valutazione di sostenibilità e impatto ex ante, l'individuazione delle tematiche di sostenibilità rilevanti connesse ai settori a cui è riferita la presente Politica, in sede di valutazione di impatto di sostenibilità dell'operazione a supporto delle strutture competenti;
- assicura l'attività di valutazione ex post dell'impatto aggregato effettivamente generato dalle iniziative poste in essere da CDP.

### **Direzione Business**

- assicura, anche avvalendosi del necessario supporto della Direzione Amministrazione, Finanza, Controllo e Sostenibilità e/o della Direzione Pubblica Amministrazione, il rispetto dei principi contenuti nel presente documento nelle operazioni di Finanziamento, anche orientando le attività di *origination* verso operazioni coerenti con quanto stabilito dalla presente Politica nonché dalla Politica Generale di Finanziamento Responsabile di CDP;
- sottopone all'approvazione del Consiglio di Amministrazione tutte le operazioni di esportazione inerenti il Settore Difesa e Sicurezza e le operazioni per le quali rilevano le casistiche di deroga, secondo quanto previsto dalla presente Politica.

### **Direzione Investimenti, Persone, Trasformazione e Relazioni Esterne**

- assicura anche avvalendosi del necessario supporto della Direzione Amministrazione, Finanza, Controllo e Sostenibilità e/o della Direzione Pubblica Amministrazione, il rispetto dei principi contenuti nel presente documento nelle operazioni di Investimento, anche orientando le attività di *origination* verso operazioni coerenti con quanto stabilito dalla presente Politica, nonché dalla Politica Generale di Investimento Responsabile di CDP;

- sottopone all'approvazione del Consiglio di Amministrazione tutte le operazioni di investimento inerenti al Settore Difesa e Sicurezza e le operazioni per le quali rilevano le casistiche di deroga, secondo quanto indicato dalla presente Politica;
- contribuisce all'individuazione delle tematiche rilevanti utili a definire le priorità strategiche attraverso il dialogo costante con gli *stakeholder* di riferimento;
- presidia, in collaborazione con le altre unità organizzative competenti, il dialogo con la società civile al fine di acquisire, monitorare ed orientare il posizionamento su tematiche rilevanti. per la definizione dei contenuti del presente documento;
- garantisce le opportune iniziative di sensibilizzazione e formazione relativamente al presente documento.

### **Direzione Rischi**

- assicura un presidio di secondo livello dei rischi per le parti di competenza, in ottemperanza ai principi della Politica Generale Rischi, della *Policy* di Gruppo Valutazione Rischio reputazionale delle operazioni, della *Policy* Antiriciclaggio e del Regolamento Indicatori di anomalia antiriciclaggio;
- assicura la valutazione dei rischi ESG.

### **Direzione Internal Audit**

- assicura un presidio di terzo livello, sulla base del proprio Regolamento approvato dal Consiglio di Amministrazione e con un approccio *risk-based*, valutando la completezza, adeguatezza, funzionalità (in termini di efficacia ed efficienza) ed affidabilità del sistema di controllo interno riferito ai processi aziendali;
- segnala tempestivamente alle strutture aziendali competenti gli elementi di criticità rilevati nelle verifiche e monitora periodicamente la corretta realizzazione delle azioni di mitigazione conseguenti.

## 6. TRASPARENZA E RENDICONTAZIONE

CDP, riconoscendo il valore della trasparenza e del dialogo continuo con i propri clienti, investitori, agenzie di *rating* e organizzazioni della società civile, al fine di comprenderne le legittime aspettative, si impegna ad una rendicontazione continua e trasparente.

A tal fine, CDP pubblica annualmente sul proprio sito web la rendicontazione di sostenibilità, in conformità con gli *European Sustainability Reporting Standards*, secondo quanto previsto dalla *Corporate Sustainability Reporting Directive*.

Il presente documento è pubblicato sul sito istituzionale di CDP.

## 7. ALLEGATI

### 7.1 Glossario

- **Agenda ONU 2030<sup>25</sup>**: programma d'azione per le persone, il pianeta e la prosperità sottoscritto nel settembre 2015 dai governi dei 193 paesi membri dell'ONU. Essa ingloba 17 Obiettivi per lo Sviluppo Sostenibile – *Sustainable Development Goals*, SDG – in un grande programma d'azione per un totale di 169 target.
- **Armi cibernetiche ("cyber weapons")**: mezzi di guerra cibernetica<sup>26</sup> progettati, utilizzati, o destinati a essere utilizzati per causare lesioni o morte a persone, oppure danni o distruzione a oggetti; in altre parole, provocano conseguenze tali da qualificare un'operazione cibernetica come un attacco<sup>27</sup>.

<sup>25</sup> <https://unric.org/it/agenda-2030/>

<sup>26</sup> L'insieme delle operazioni militari condotte nel e tramite il Cyberspazio per infliggere danni all'avversario, statale o non, consistenti – tra l'altro – nell'impedirgli l'utilizzo efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del Cyberspazio) – fonte: Agenzia per la Cybersicurezza Nazionale.

<sup>27</sup> Fonte: Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, Rule 103, par.2, pag. 452. Il Tallinn Manual è stato redatto su iniziativa del NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), un centro di eccellenza NATO con sede a Tallinn, Estonia.

Per maggiori informazioni, si veda la pagina ufficiale del CCDCOE dedicata al Tallinn Manual: <https://ccdcoe.org/research/tallinn-manual/>

- **Armi comuni da sparo:** armi di cui all'art. 2 legge 110/75, comprende fucili e carabine che, pur potendosi prestare all'utilizzazione del munizionamento da guerra, presentino specifiche caratteristiche per l'effettivo impiego per uso di caccia o sportivo, abbiano limitato volume di fuoco e siano destinate ad utilizzare munizioni di tipo diverso da quelle militari. Costituiscono armi comuni da sparo: i fucili anche semiautomatici con una o più canne ad anima liscia; i fucili con due canne ad anima rigata, a caricamento successivo con azione manuale; i fucili con due o tre canne miste, ad anime lisce o rigate, a caricamento successivo con azione manuale; i fucili, le carabine ed i moschetti ad una canna ad anima rigata, anche se predisposti per il funzionamento semiautomatico; i fucili e le carabine che impiegano munizioni a percussione anulare, purché non a funzionamento automatico; le rivoltelle a rotazione; le pistole a funzionamento semiautomatico. Si intendono incluse anche le munizioni ed esplosivi per armi leggere e di piccolo calibro.
- **Armi controverse:** armi che hanno effetti indiscriminati e causano indebitamente danni e lesioni. L'insieme di tali armi può variare nel corso del tempo a causa di possibili sviluppi tecnologici. Alla data di pubblicazione della presente Politica e ai fini dell'applicazione della stessa, sono considerate armi controverse le seguenti:
  - **armi nucleari** - dispositivi in grado di rilasciare energia nucleare in maniera incontrollata e che hanno una serie di caratteristiche che li rendono idonei a essere utilizzati per finalità belliche (definizione del Trattato di non proliferazione delle Armi nucleari in America Latina e nei Caraibi del 1967);
  - **armi chimiche** - si definiscono tali:
    - a. armi usate in combattimento che utilizzano le proprietà tossiche di alcune sostanze chimiche, per uccidere, ferire o comunque mettere fuori combattimento il nemico;
    - b. munizioni e dispositivi o sistemi progettati specificamente per uccidere o provocare ferite utilizzando le proprietà tossiche delle sostanze chimiche;
    - c. qualunque attrezzatura specificamente progettata per essere utilizzata direttamente assieme alle munizioni e ai dispositivi specificati.

Esse sono regolamentate dalla Convenzione sulle Armi Chimiche del 1993 (CAC), trattato sul disarmo delle Armi chimiche che ne inibisce qualsiasi attività volta allo sviluppo, produzione, acquisizione, detenzione, conservazione, trasferimento.

- **armi biologiche** - si definiscono tali:
  - a. agenti microbiologici nocivi o tossine da essi prodotte, utilizzate come strumento di offesa, ovvero la cui produzione è effettuata in quantità tali da non essere giustificate per finalità di profilassi, di protezione o pacifiche;
  - b. armi, attrezzature o mezzi progettati per utilizzare tali agenti o tossine per finalità ostili. Gli agenti biologici utilizzati per la loro realizzazione si dividono in: virali (ad es. febbre gialla), batteriologici (ad es. peste), biologici ad effetto indiretto.

Esse sono regolamentate dalla Convenzione per le Armi biologiche del 1972 (*Biological and Toxin Weapon Convention – BTWC*);

- **armi all'uranio impoverito** - l'uranio impoverito è ottenuto come scarto del procedimento di arricchimento dell'uranio. È utilizzato nella produzione di munizioni anticarro per la sua efficacia contro le corazzature. Non è regolamentato da nessuna convenzione internazionale ma CDP annovera tali materiali tra quelli esclusi dall'operatività, al pari delle Armi controverse;
- **mine anti-persona** - mina progettata in modo tale da esplodere alla presenza, prossimità o contatto con una persona e tale da incapacitare, ferire o uccidere una o più persone (ai sensi dell'articolo 2, commi 1 e 2, della Convenzione sul divieto d'impiego, di stoccaggio, di produzione e di trasferimento delle mine antipersona e sulla loro distruzione, firmata a Ottawa il 3 dicembre 1997, ratificata con legge 26 marzo 1999, n. 106. La stessa definizione è richiamata dalla legge 220/2021 recante "Misure per contrastare il finanziamento delle imprese produttrici di mine antipersona, di munizioni e submunizioni a grappolo"). Le mine progettate per essere detonate dalla presenza, prossimità o contatto di un veicolo, invece che di una persona, e dotate di dispositivi di anti-manipolazione, non sono considerate mine antipersona per il solo fatto di essere così congegnate;
- **mine anti-carro:** armi con lo scopo di distruggere o danneggiare carri armati e altri veicoli;
- **munizioni e submunizioni cluster / bombe o munizioni a grappolo** - munizione convenzionale idonea a disperdere o rilasciare submunizioni esplosive ciascuna di peso inferiore a 20 chilogrammi, fatte salve le specifiche di esclusione indicate dalle lettere a), b) e c) del comma 2, articolo 2 della Convenzione di Oslo sulla messa al bando delle munizioni a grappolo, fatta a Dublino il 30 maggio 2008, di cui alla legge 14 giugno 2011, n. 95. La definizione è ripresa anche dalla legge 220/2021 recante "Misure per contrastare il finanziamento delle imprese produttrici di mine antipersona, di munizioni e submunizioni a grappolo".
- **Armi di piccolo calibro:** armi ad uso singolo quali ad esempio: revolver e pistole autocaricanti, fucili e carabine, fucili d'assalto e mitragliatrici leggere. Si intendono incluse anche le munizioni ed esplosivi per armi di piccolo calibro.
- **Armi leggere:** sono generalmente definite come armi collettive progettate per essere utilizzate da due o tre persone, sebbene alcune possano essere portate e utilizzate da una sola persona, quali ad esempio: mitragliatrici pesanti, lanciamissili anticarro portatili e

lanciarazzi, lanciamissili antiaerei portatili. Si intendono incluse anche le munizioni ed esplosivi per armi leggere.

- **Cybersicurezza (“Cybersecurity”)**: preservazione della riservatezza, integrità e disponibilità di informazioni nel Cyberspazio, quest'ultimo inteso come l'ambiente complesso risultante dall'interazione di persone, *software* e servizi su Internet per mezzo di dispositivi tecnologici e reti ad essi connessi<sup>28</sup>.
- **Controparte**: Società beneficiaria del Finanziamento o dell'Investimento. Nel caso di operazioni di: (i) esportazione come Controparte si intende la società promotrice/esportatore dell'operazione; (ii) *project financing* come Controparte si intendono sia il *borrower*/ SPV che gli azionisti di quest'ultima che detengono singolarmente o congiuntamente una partecipazione (pari ad almeno il 51% del capitale).
- **Environmental, Social and Governance (ESG)**: indica i fattori di tipo ambientale, sociale e di governo societario che qualificano una attività finanziaria come sostenibile.
- **Finanziamento**: senza pregiudizio per le altre normative interne/di Gruppo collegate, ai fini del presente documento indica la tipologia di impiego con scopo generico o scopo specifico, comprendente le attività effettuate sotto qualsiasi forma tecnica consentita dalla legge e dallo Statuto di CDP con fondi propri e con fondi di terze parti, sia a livello domestico sia internazionale, ivi inclusi i prestiti obbligazionari, le linee di credito *revolving*, l'acquisto di crediti di impresa e il rilascio di garanzie<sup>29</sup>.
- **Gruppo CDP**: Cassa Depositi e Prestiti S.p.A. e Società soggette a direzione e coordinamento di CDP S.p.A. ai sensi degli articoli 2497 e seguenti del Codice civile.
- **Investimento**: senza pregiudizio per le altre normative interne/di Gruppo collegate, ai fini del presente documento, indica l'attività di investimento effettuata sia attraverso investimenti diretti (investimenti in azioni, quote e/o titoli rappresentativi del capitale di rischio di società, strumenti finanziari partecipativi in società, altri strumenti, anche ibridi, simili nella sostanza economica a quelli precedenti, sia a livello domestico sia internazionale, o investimenti immobiliari), che attraverso investimenti indiretti (investimenti in quote di fondi comuni di investimento di debito ed *equity* o fondi di fondi gestiti da Società di Gestione del Risparmio (SGR) e partecipazioni in altri OICR (Organismi di Investimento Collettivo del Risparmio) o in altri veicoli di investimento, sia a livello domestico sia internazionale), con fondi propri e con fondi di terze parti<sup>30</sup>.
- **Malware**: contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo<sup>31</sup>.
- **Materiali di armamento**: materiali che, per requisiti o caratteristiche tecnico-costruttive o di progettazione, sono tali da considerarsi costruiti per un prevalente uso militare o di corpi armati o di polizia, così come definiti dall'art. 2 della legge 185/90 e s.m.i, e classificati nelle seguenti categorie:
  - Armi nucleari, biologiche, chimiche ed elettriche
  - Armi da fuoco automatiche e relativo munizionamento
  - Armi ed armamenti di medio e grosso calibro e relativo munizionamento
  - Bombe, torpedini, mine, razzi, missili e siluri
  - Carri e veicoli appositamente costruiti per uso militare
  - Navi e relativi equipaggiamenti appositamente costruiti per uso militare
  - Aeromobili ed elicotteri e relativi equipaggiamenti appositamente costruiti per uso militare
  - Polveri, esplosivi, propellenti
  - Sistemi o apparati elettronici, elettroottici e fotografici appositamente costruiti per uso militare
  - Materiali speciali blindati appositamente costruiti per uso militare
  - Materiali specifici per l'addestramento militare
  - Macchine, apparecchiature ed attrezzature costruite per la fabbricazione, il collaudo ed il controllo delle armi e delle munizioni
  - Equipaggiamenti speciali appositamente costruiti per uso militare.
- **Merci praticamente utilizzabili solo per la pena di morte, per la tortura o per altri trattamenti o pene crudeli, inumani o degradanti**: merci individuate dal Regolamento (UE) 2019/125 e che rappresentano attrezzature che hanno come scopi principali la pena di morte, la tortura o altri trattamenti o pene crudeli, inumani o degradanti, come ad esempio le merci destinate all'esecuzione o contenzione di esseri umani.

<sup>28</sup> Fonte: ISO 27001

<sup>29</sup> Per informazioni sulle Operazioni di Finanziamento a cui si applica la presente Politica, si rimanda al paragrafo 3.1 “Perimetro per tipologia di operazione”.

<sup>30</sup> Per informazioni sulle Operazioni di Investimento a cui si applica la presente Politica, si rimanda al paragrafo 3.1 “Perimetro per tipologia di operazione”.

<sup>31</sup> Fonte: Glossario Agenzia per la Cybersicurezza Nazionale.

- **Obiettivi di sviluppo sostenibile (SDG):** 17 obiettivi concordati dall'Organizzazione delle Nazioni Unite che mirano a raggiungere complessivamente 169 target riguardanti lo sviluppo economico e sociale, tra cui la povertà, la fame, la salute, l'istruzione, il cambiamento climatico, l'uguaglianza di genere, l'acqua, i servizi igienico-sanitari, l'energia, l'urbanizzazione, l'ambiente e l'uguaglianza sociale.
- **Prodotti a duplice uso (c.d. beni *dual use*):** prodotti, inclusi il *software* e le tecnologie, che possono avere un utilizzo sia civile sia militare e comprendono i prodotti che possono essere impiegati per la progettazione, lo sviluppo, la produzione o l'uso di armi nucleari, chimiche o biologiche o dei loro vettori, compresi tutti i prodotti che possono avere sia un utilizzo non esplosivo sia un qualsiasi impiego nella fabbricazione di armi nucleari o di altri ordigni esplosivi nucleari (Art. 2 del Regolamento (UE) 2021/821), come dall'elenco di cui all'Allegato I del Regolamento (UE) 2021/821.
- **Piano Strategico:** Piano Strategico 2025-2027 del Gruppo CDP, approvato dal Consiglio di Amministrazione di CDP nella seduta del 19 dicembre 2024, inclusivo di eventuali successivi aggiornamenti.
- **Ransomware:** *malware* che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I *ransomware* sono, nella maggioranza dei casi, dei *trojan* diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica<sup>32</sup>. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamenti ed altri oggetti simili.
- **Settore della Difesa e Sicurezza:** settore inerente la produzione e commercializzazione di armi, materiali di armamento, beni *dual use* collegati all'utilizzo nel settore, inclusi i prodotti o servizi inerenti la *Cybersecurity*.

La Politica di prima emanazione è stata approvata dal CdA in data 14 dicembre 2022 e il presente aggiornamento è stato approvato dal CdA in data 20 novembre 2025

<sup>32</sup> Fonte: Glossario Agenzia per la Cybersecurity Nazionale