Einschätzung zum Dummy-Verfahren aus fachlicher Sicht:

I. Fragliche Aspekte mit Blick auf eine substantiierte rechtliche Begründung nach der Maßgabe der bisherigen Rechtsprechung:

1. Grundsätzlich ist anzumerken, dass entsprechend unserer bisherigen Einlassung aus Sicht der BNetzA entscheidend war und ist, dass die Empfehlungen des Prüfungsausschusses sowohl hinsichtlich der Sachverhaltsaufklärung als auch hinsichtlich der rechtlichen Würdigung ausreichend substantiiert gestaltet sein müssen, um eine Stellungnahme der BNetzA – ohne vertiefte eigene Sachverhaltsrecherche und komplexe eigene Aufarbeitung der fallbezogenen bisherigen urheberrechtlichen Rechtsprechung - zu ermöglichen. Dementsprechend hoch ist die Erwartungshaltung an die Ausführlichkeit der Empfehlung. Das aktuelle Dummy-Verfahren und die übermittelte Empfehlung wirft diesbezügliche Zweifel auf, da die Empfehlung des Prüfausschusses sehr kurz gehalten ist und an vielerlei Stellen lediglich Feststellungen trifft, ohne dass diese dezidiert begründet, insbesondere nicht mit der relevanten zugrundeliegenden Rechtsprechung unterlegt werden.
2. Nach Durchsicht der Empfehlung waren vertiefte BNetzA-eigene Recherchen relevanter urheberrechtlicher Entscheidungen notwendig, um nachvollziehen zu können, dass die in der Empfehlung angeführten Aspekte (wie z.B. „hat kein Impressum“) auf bisherige Entscheidungen nationaler Gerichte zurückgehen. Diese sorgfältige Eigenrecherche der zugrunde gelegten Rechtsprechung durch die BNetzA ist zeitaufwendig und läuft den Interessen des Roundtable zuwider, von der BNetzA (zumindest mittelfristig) formlose Stellungnahmen zu 12 Empfehlungen der Clearingstelle im Monat zu erhalten.
3. Nur substantiierte und mit entsprechenden Verweisen auf die relevante Rechtsprechung versehene Ausführungen erleichtern es der BNetzA, die geplante Plausibilitätsprüfung durchzuführen. Sie sind für die beabsichtigte Einbeziehung der BNetzA unerlässlich. Entsprechende Verweise auf die Rechtsprechung sind in der Empfehlung im Dummy-Verfahren lediglich hinsichtlich der Rechtsgrundlage (Störerhaftung/§ 7 Abs. 4 TMG direkt oder analog/RL-Recht direkt/Rundfunkstaatsvertrag) angegeben. Sodann wird lediglich – ohne Begründung – auf § 7 Abs. 4 TMG abgestellt (was im Ergebnis aus Sicht der BNetzA keinen Bedenken begegnet).
4. Weitere Gesichtspunkte, die als rechtliche Voraussetzung des § 7 Abs. 4 TMG nachgewiesen werden müssten, werden lediglich „behauptet“ oder festgestellt – ebenfalls ohne weitere rechtliche Begründung. So werden etwa zum Nachweis der Aktivlegitimation ein Wikipedi-Eintrag bzw. die Nennung im Abspann des Filmwerks angeführt, ohne dass weiter ausgeführt wird, warum diese Aspekte als rechtliche Ansatzpunkte für die entsprechende Aktivlegitimation ausreichend sind. Im Weiteren wird daraus abgeleitet, dass damit die Antragstellerin „im Zweifel“ über das ausschließliche Nutzungsrecht verfüge. Anhaltspunkte, die dem entgegenstehen, lägen nicht vor.
5. Aus hiesiger Sicht ist es unerlässlich, in die Empfehlungen der Clearingstelle weitergehende Begründungen und Herleitungen sowie Verweise auf die zugrundeliegende Rechtsprechung aufzunehmen, um eine Stellungnahme zur Annahme einer Ausnahme im Sinne des Art. 3 Abs. 3 UAbs. 3 a TSM-VO abgeben zu können.

II. Fragliche Aspekte mit Blick auf die substantiierten relevanten Nachweise, insb. technischer Abläufe:

1. INCOPRO ist ein Unternehmen, welches nach eigener Aussage Technologie betreibt, um Urheberrechtsverletzungen aufzuspüren (Anlage II - Evidence Pack, S. 2).

Deren Recherche-System „Identify“ spürt Websites auf, die angeblich urheberrechtlich geschützte Werke unrechtmäßig veröffentlichen. Dies ist eine „Unterstellung“, die sich automatisiert nicht feststellen lässt. Denn es kann automatisiert nicht zweifelsfrei erkannt werden, ob ein Inhalt tatsächlich ohne Lizenz verbreitet wird.

2. Es wurden unterschiedliche Domains identifiziert. Geprüft wurde laut der beigelegten Screenshots jedoch nur eine der Domains.
3. Die Aussage „The site immediately advises users to use a DNS resolver from Google or Cloudflare to hide their IP address when streaming unlawful content“ (Anlage II – Evidence Pack, S. 10) lässt auf fehlende Sachkenntnis über das Domain Name System (DNS) und die Mechanismen zur Auflösung von Domainnamen schließen. Es ist technisch unmöglich, mittels DNS-Resolver eine IP-Adresse (Sender oder Empfänger) zu verschleiern. Die IP-Adressen in IP-Datenpaketen bleiben auch bei Benutzung eines DNS-Resolver unverändert. Die Unkenntnis über elementare Funktionen des DNS und damit des zentralen Gegenstands von Websperren mittels DNS-Sperren lässt Zweifel an der Fachkompetenz des Unternehmens INCORPRO aufkommen.
   Der Hinweis auf dem Screenshot der Website rät lediglich, die DNS-Resolver von Google (mit den IP-Adressen 8.8.8.8 und 8.8.4.4) zu nutzen, um eventuelle DNS-Sperren zu umgehen. Ein Hinweis auf DNS-Resolver von Cloudflare – wie von INCORPO dargestellt – erfolgt nicht.
   Aus der Empfehlung zur Nutzung des Google-DNS lässt sich auch nicht auf einen Vorsatz zur Urheberrechtsverletzung schließen, es gibt zahlreiche andere Gründe zur Nutzung eines alternativen DNS, z. B. Leistungsfähigkeit/Geschwindigkeit, Datenschutz oder Umgehung von Zensur durch totalitäre Regime.
4. Recherche zu tatsächlichen Betreibern der Websites, Hoster der Websites und Domain-Inhaber der Websites ist nicht erschöpfend (Anlage II – Evidence Pack, S. 12)
   a. Die Website hat kein Impressum, es wurde eine Kontaktaufnahme per Supportforum versucht bzw. es wurde einmal eine E-Mail an contact@s.to geschickt, welche als Ticket im Support-Forum eingegangen ist. Weitergehende Kontaktversuche wurden nicht aufgeführt.
   b. Weitere Versuche, die Betreiber der Websites über die Domain-Registrare herauszufinden, wurden anscheinend nicht durchgeführt. Beispielsweise wurde in den beigelegten Screenshots nur Recherche zur Domain „s.to“, nicht aber zu den beiden anderen aufgeführten Domains belegt. Eine Recherche beim Domain-Registrar für „sx“-Domains, www.whois.sx, hätte vielleicht zu Erfolg führen können, da dort diverse Daten aus Datenschutzgründen nicht veröffentlicht wurden, jedoch bei einer begründeten Anfrage ggf. herausgegeben worden wären.
   c. Versuche, über andere Wege (Beispielsweise über die Aussteller des TLS-Zertifikates der Webseite) Informationen über den Website-Betreiber oder Hoster zu erlangen, wurden anscheinend nicht durchgeführt.
   d. Die Identifizierung des (vermeintlichen) Hosters der Website wurde durch „who-is“-Abfrage von „domaintools.com“ durchgeführt. IP-Adressen für Europa, den Nahen Osten und Zentralasien werden alleinig durch RIPE verwaltet und vergeben. Es ist verwunderlich, dass nicht die originäre (und verbindliche) WHOIS-Datenbank von RIPE für die Abfrage benutzt wurde. Stattdessen wird die Datenbank eines Drittanbieters verwendet, von dem Aktualität und Genauigkeit der Daten nicht nachvollziehbar sind. Abfragen über RIPE (oder andere offiziellen Internet-Registrare) sind grundsätzlich solchen über Drittanbieter (die ggf. einen veralteten Datenbestand haben) vorzuziehen.

(Das gezeigte Vorgehen von INCOPRO lässt Zweifel der Sachkenntnis aufkommen.)

Eine RIPE-Abfrage durch die BNetzA liefert u.a. die folgenden Daten:

person: [redacted]
address: Russia, Rostov-on-Don
phone: [redacted]
e-mail: [redacted]

sowie

role: DDoS-Guard.NET NOC
address: Russia, Rostov-on-Don
e-mail: noc@ddos-guard.net

Anscheinend wurden diese Informationen von INCOPRO nicht genutzt und nicht versucht, mittels dieser Adressdaten, einen Kontakt mit dem Verantwortlichen Betreiber von s.to aufzunehmen.

e. Darüber hinaus wurde über die WHOIS-Abfrage als Hoster „ddos-guard“ identifiziert und ein „Hosting outside of Germany“ unterstellt (Anlage II – Evidence Pack, S. 13). An gleicher Stelle wird jedoch auch aufgeführt, dass ddos-guard auch CDN-Dienste anbietet. Darüber hinaus ist ddos-guard Anbieter weiterer Absicherung von Websites vor Angriffen. Somit lassen die vorgelegten Informationen nicht den Schluss zu, dass ddos-guard der Hosting-Betreiber der Webseite ist.

Aus technischer Sicht lassen WHOIS-Datenbank-Abfragen grundsätzlich nur den Rückschluss zu, welcher Person die analysierte IP-Adresse zugewiesen wurde und welchem AS (Autonomous System; ein autark betriebenes Netz, das Teil des Internetnetzverbundes ist) diese zuzuordnen ist. Allein aus diesen Daten kann kein Rückschluss auf den tatsächlichen Host der Webseite geschlossen werden. Hierzu wären weitere Information notwendig, z.B. dass belegt wird, dass das AS262254 ausschließlich von dessen Betreiber für Hostingzwecke eingesetzt wird.

WHOIS-Datenbank-Abfragen stellen nur einen ersten Hinweis dar, der aber weitere Untersuchungen nach sich ziehen muss.